Vysoká škola báňská - Technická univerzita Ostrava

Fakulta bezpečnostního inženýrství

Katedra bezpečnostního managementu

Použití biometrické identifikace při zabezpečení objektu

Student: Petik Lukáš
Vedoucí bakalářské práce: Mgr. Ing. Radomír Ščurek, Ph.D.

Studijní obor: Technická bezpečnost osob a majetku
Datum zadání bakalářské práce: 20. října 2007
Termín odevzdání bakalářské práce: 30. dubna 2008

Zadání bakalářské práce

Student: **Petik Lukáš**
Studijní program: B3908 Požární ochrana a průmyslová bezpečnost
Studijní obor: 3908R005 Technická bezpečnost osob a majetku

Vedoucí katedry Vám v souladu se Studijním a zkušebním řádem pro studium v bakalářských studijních programech Vysoké školy báňské – technické univerzity Ostrava určuje tuto bakalářskou práci:

Název tématu: **Použití biometrické identifikace při zabezpečování objektu**
Anglický název: **The Use of Biometric Identification to Secure the Building**
Cíl práce: Zjistit a popsat aktuální technologie a systémy spojené s biometrickou identifikací osob. Na základě teoretických znalostí a praktických poznatků navrhnout na imaginárním objektu zabezpečení jeho vstupu a identifikaci osob vstupujících do chráněných prostor.

Charakteristika práce:

- Popis zadané problematiky, základní východiska
- Teorie autentizace v přístupových systémech
- Technologické a fyzikální principy biometrických senzorů
- Rozbor funkcí a logických přístupů konkrétních snímačů, rozpoznávací algoritmy otisku prstu
- Zabezpečení vstupu do objektu současnými prostředky technické ochrany objektu, nové metody a organizační postupy
- Trendy vývoje a srovnání biometrických snímačů u nás a v zahraničí
- Návrh optimálního řešení ochrany vstupních prostor do objektu

Základní literární prameny:

- Jain, A.; Bolle, R.; Pankanti, S: Biometrics: Personal identification in networked society, Kluwer Academic Publisher, 1999
- Sandström, M.: Liveness detection in fingerprint recognition systems, 2004
- Soumar, C.: Biometric system security, Secure - The silicon trust quaterly report, 01/2002, 46-49.
- Bromba, M.: Bioidentification, 2007
- Galbavý, M.: Vizualizace a vzdálené řízení v síti Longworks, České vysoké učení technické v Praze, 2006
- Křeček, S.: Příručka zabezpečovací techniky, Praha, 2002
- Toms, L., Koníček, T., Kocábek, P.: Zabezpečení dveří a oken – rizikových míst objektů. MV ČR, odbor prevence kriminality, Praha, 1997
- Večerka, K. a kol.: Prevence kriminality v teorii praxi. IKSP, Praha, 1996
- Brabec, F. a kol.: Bezpečnost pro firmu, úřad, občana. Public History, Praha, 2001.
- ČSN P ENV 1627 Okna, dveře, uzávěry – odolnost proti násilnému vniknutí. Požadavky a klasifikace, 2000. Český normalizační institut
- ČSN EN 50131-1: Poplachové systémy – Elektrické zabezpečovací systémy uvnitř a vně budov. Část 1: Všeobecné požadavky, 1999, Změna Z1:2000, Český normalizační institut
- Vyhlášky č. 339/1999 Sb., o objektové bezpečnosti
- Sborníky odborných konferencí a seminářů

Vedoucí bakalářské práce: Mgr. Ing. Radomír Ščurek, Ph.D.

Konzultant bakalářské práce:

Termín odevzdání bakalářské práce: 30. dubna 2007

ANOTACE

PETIK, Lukáš. ***Použití biometrické identifikace při zabezpečení objektu*****. Bakalářská práce, Ostrava 2008**

Práce poskytuje kompletní přehled současných technologických metod a přístupů při identifikaci osob na základě biometrického prvku. Pozornost je věnována především biometrické identifikaci dle otisku prstu, dnes stále ještě nejrozšířenějšímu principu. Dále se práce zabývá problematikou zabezpečením budov a především identifikací uživatelů vstupujících do chráněných prostor. Navržené zabezpečení bylo implementováno na imaginárním modelu administrativní budovy. K zabezpečení vstupu do objektu byl využit snímač otisků prstů od firmy Synel.

Klíčová slova

biometrie, autentifikace, verifikace, identifikace, senzor, markanta

ANNOTATION

PETIK, Lukáš. ***The Use of Biometric Identification to Secure Building*****. Bachelor thesis, Ostrava 2008**

This work provides complete survey of current technological methods and views on person identification by virtue of biometric element. The attention is given to biometric identification based on fingerprint, because it's still the most expanded technology. In the next part, there is the thesis focus on problems of buildings security and especially on possibilities of identification users incoming to the protected area. Designed security of protected areas was implemented on imaginary model of administration building. To security of entry to building was used fingerprint scanner from company Synel.

Keywords

biometric, authentication, verification, identification, sensor, minutia

Poděkování

Dovoluji si poděkovat Mgr. Ing. Radomíru Ščurkovi Ph.D. za pomoc, kterou mi poskytl při vypracování bakalářské práce i za odborné konzultace.

V Ostravě dne 11.dubna 2008 .....

podpis

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, zákony atd.) uvedené v přiloženém seznamu.

Nemám závažný důvod proti použití tohoto školního díla ve smyslu § 60 zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Ostravě dne 11.dubna 2008 .....

podpis

OBSAH

1 Úvod

V současné společnosti se čím dál více klade důraz na bezpečnost objektu, na jeho ochranu a znemožnění kompromitace objektu narušením jeho střežených prostor neoprávněným uživatelem. K dosažení těchto cílů u soukromých objektů lze použít širokou škálu bezpečnostních technologických opatření, ovšem nejnovější systémy jsou budovány na základě začlenění ověřování jedinečné biologické či behaviorální vlastnosti a tím jednoznačné definice osob vstupujících do těchto chráněných prostor objektu. Mluvíme o tzv. automatických biometrických systémech řízení a kontroly vstupů.

Cílem práce je zjistit a prozkoumat existující prostředky, metody a postupy v daném oboru a vysvětlit jejich specifičnost při zabezpečení vstupních prostor do objektu, tedy nejčastějšího místa průniku nežádoucích osob. Pomocí analytických metod budou identifikovaná nebezpečí a stanovena jejich rizikovost pro bezpečnost objektu administrativní budovy. Na základě výsledků budou navržena opatření pro dosažení optimálního zabezpečení. Pozornost je věnována jednotlivým biometrický metodám, dostupným snímacím zařízením a automatickým systémům členěných dle konkrétních měřitelných biometrických vlastností. Práce se věnuje pouze komerčně dostupným systémům a neřešení biometrické systémy používané státními institucemi, především proto že jsou pro soukromé firmy finančně nedostupné. Jelikož v České republice neexistují samostatné právní předpisy či technické normy věnující se této problematice, je rozšiřování biometrických systémů u nás ponecháno na zahraničních exportních společnostech, které je poskytují na český trh prostřednictvím distributorů a obchodním zastoupením. Celkově je u nás téma automatických biometrických systémů použitelných i v komerční sféře podceňováno a neexistuje příliš vědeckých prací, které by se biometrií obecně věnovaly. Proto jsou informace v této práci unikátní nejméně tím, že jsou čerpány především ze zahraničních zdrojů a existujících vědeckých prací (státních organizací, univerzit, cizojazyčných publikací).

2 Právní úprava ochrany objektů

V kapitole jsou popsány existující právní normy a technické normy zabývající se v různých oblastech společenských vztahů ochranou a zabezpečením objektu, právem člověka na život, osobní svobodu a majetek.

2.1 Právní normy

Právní normy jsou základním prvkem systému práva vyjadřujícím závazné obecné pravidlo chování, které pro povinný subjekt představuje nejen určitou povinnost, ale i vědomost o skutečnosti, že v případě nesplnění této povinnosti subjektem nastoupí vůči němu státní donucení.

Ústava České republiky

Ústava České republiky, tedy zákon č. 1/1993 Sb., je sestavena z VIII hlav a preambule. Ústava sestává ze základních ustanovení, stanovení moci zákonodárné, stanovení moci výkonné, stanovení moci soudní, stanovení Nejvyššího kontrolního úřadu, stanovení České národní banky a územní samosprávy ČR. V čl. 1 Ústavy ČR se říká, že Česká republika je svrchovaný, jednotný a demokratický stát založený na úctě k právům a svobodám člověka a občana. Tedy i k právům vlastnit majetek a k právům na život, což dále specifikuje Listina základních práv a svobod. [21]

Listina základních práv a svobod

Dalším již uvedeným ústavním zákonem je Listina základních práv a svobod, která je součásti ústavního pořádku České republiky (zákon č. 2/1993 Sb.), od níž se odvozují následující právní úpravy. Lidská práva a svobody jsou všeobecnou a nedotknutelnou hodnotou, je uznávána nezrušitelnost přirozených práv člověka, jakožto občana a svrchovanost zákona. Zakotvuje se zde princip, že omezení základních práv a svobod je možné jen pouze na základě zákona. Listina základních práv a svobod mimo jiné garantuje: právo na život (čl. 6). V rámci řešené problematiky se vztahuje k ochraně života osob nacházejících se v chráněném objektu nebo podniku či v souvislosti se zajišťováním ochrany jiných bezpečnostních zájmů podniku; nedotknutelnost osoby a jejího soukromí (čl. 7) a osobní svobodu, (čl. 8); právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a na ochranu jména, jakož i ochranu při nedovoleném zasahování do soukromí neoprávněným shromažďováním, zveřejňováním nebo zneužíváním údajů o své osobě (čl. 10); právo vlastnit majetek (čl. 11), resp. z tohoto článku vyplývá, že vlastní-li někdo majetek, pak ostatní mají povinnost tato majetková práva respektovat; nedotknutelnost obydlí (čl. 12), není dovoleno do něj vstoupit bez souhlasu toho, kdo v něm bydlí. [22]

Ústavní zákon o bezpečnosti České republiky

Jedná se o zákon č. 110/1998 Sb., ve znění pozdějších předpisů. Stanovuje, že základní povinností státu je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot. [17]

Občanský zákoník

Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů uvádí, že vlastník je v mezích zákona oprávněn předmět svého vlastnictví držet, používat jeho plody a užitky a nakládat s ním (§ 123). Vlastník má právo na ochranu proti tomu, kdo do jeho vlastnických práv neoprávněně zasahuje (§ 126). Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy (§ 11). Jestliže hrozí neoprávněný zásah do práv bezprostředně, může jej ten, kdo je takto ohrožen, přiměřeným způsobem zásah sám odvrátit (§ 6). Každý je povinen počínat si tak, aby nedošlo ke škodám na zdraví, na majetku (§ 415). Komu hrozí škoda, je povinen k jejímu odvrácení zakročit způsobem přiměřeným okolnostem ohrožení (§ 417). Kdo způsobil škodu, když odvracel přímo hrozící nebezpečí, které sám nevyvolal, není za ni odpovědný, ledaže bylo možno toto nebezpečí za daných okolností odvrátit jinak, anebo jestliže je způsobený následek zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil. Rovněž neodpovídá za škodu, kdo ji způsobil v nutné obraně proti hrozícímu nebo trvajícímu útoku (§ 418). Každý odpovídá za škodu, kterou způsobil porušením právní povinnosti. Odpovědnosti se zprostí ten, kdo prokáže, že škodu nezavinil (§ 420). [17]

Trestní zákoník

Zákon č. 140/1961 Sb., trestní zákon ve znění pozdějších předpisů, jeho účelem je chránit zájmy společnosti, ústavní zřízení České republiky, práva a oprávněné zájmy fyzických a právnických osob. Popisuje některé okolnosti vylučující protiprávnost. Jde zejména o:

Nutnou obranu (§ 13): „Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvající útok na zájem chráněný tímto zákonem, není trestným činem“. K jednání v nutné obraně je

oprávněn jednat kdokoliv, musí jít však o útok, nebo hrozbu útoku ze strany člověka a útok musí přímo hrozit nebo trvat.

Krajní nouzi (§14): „Čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněného tímto zákonem, není trestným činem. Nejde o krajní nouzi, jestliže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo způsobený následek je zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil.“ Kdokoliv je oprávněn jednat v krajní nouzi, odvrací-li nebezpečí, které přímo hrozí zájmu chráněném trestním.

Oprávněné použití zbraně (§ 15): „Trestný čin nespáchá ten, kdo použije v mezích zmocnění příslušných zákonných předpisů.“ Týká se určitých osob (voják, policista a další).

K okolnostem vylučující protiprávnost dále patří svolení poškozeného na základě občanského zákoníku. Jednání je dovolené, jestliže se jedná o zájmy, o nichž může poškozený sám rozhodovat a netýká se to zájmu společnosti a ostatních občanů. Svolení se zpravidla týká majetku ve vlastnictví občanů. Další okolností je plnění zákonné povinnosti nebo rozkazu, výkon práva a povolání, riziko ve výrobě a výzkumu a lékařský zákrok podle nejnovějších poznatků lékařské vědy (například amputace).

Paragrafy Trestního zákoníku vztahující se k ochraně osob a objektu:

§ 234 Loupež: „Kdo proti jinému užije násilí nebo pohrůžky bezprostředního násilí v úmyslu zmocnit se cizí věci, bude potrestán odnětím svobody.“

§ 238 Porušování domovní svobody: „Kdo neoprávněně vnikne do domu nebo do bytu jiného nebo tam neoprávněně setrvá, bude potrestán odnětím svobody.“

§ 247 Krádež: „ Kdo si přisvojí cizí věc tím, že se jí zmocní bude potrestán.“

§ 257 Poškozování cizí věci: „ Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci. [24]

Trestní řád

Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů, v § 76 odst. 2 uvádí, že kdokoliv (pracovník soukromé či podnikové bezpečnostní služby stejně, jako kterýkoliv jiný občan) může osobu, která byla přistižena při trestném činu, zadržet, je-li to nezbytně třeba k zajištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen zadrženou osobu neprodleně odevzdat státnímu zástupci

vyšetřovateli, vyhledávacímu orgánu, orgánu policie, nebo u příslušníka ozbrojených sil, správci posádky. Nelze-li takovou osobu ihned předat, je třeba některému z uvedených orgánů omezení osobní svobody bez odkladu oznámit. [25]

Zákon o ochraně utajovaných informací a personální bezpečnosti

Zákon č. 412/2005 Sb., ve znění pozdějších předpisů, definuje utajovanou informaci jako skutečnost, se kterou by neoprávněné nakládání mohlo způsobit újmu zájmům České republiky nebo zájmům, k jejichž ochraně se Česká republika zavázala, nebo by mohlo být pro tyto zájmy nevýhodné a která je uvedena v seznamu utajovaných informací. Zákon zařazuje utajované informace do čtyř stupňů utajení: přísně tajné, tajné, důvěrné, vyhrazené. Tento zákon vymezuje hlavní oblasti, ve kterých se utajované informace vyskytují a stanoví povinnosti, jak s nimi mají organizace a fyzické osoby nakládat. Zabývá se ochranou osob, objektů a předmětů a specifikuje zabezpečení objektů kombinací bezpečnostních opatření, jako je fyzická ochrana, technické prostředky, režimové a administrativní opatření a další. [17]

Zákoník práce

Zákon č. 262/2006 Sb., ve znění pozdějších předpisů, definuje v části páté, hlavě I., povinnosti zaměstnavatele vytvářet podmínky pro bezpečné, nezávadné a zdraví neohrožující pracovní prostředí vhodnou organizací bezpečnosti a ochrany zdraví při práci a přijímáním opatření k prevenci rizik (§ 101). Prevencí rizik se zde rozumí všechna opatření vyplývající z právních a ostatních předpisů k zajištění bezpečnosti a ochrany zdraví při práci a z opatření zaměstnavatele, která mají za cíl předcházet rizikům, odstraňovat je nebo minimalizovat působení neodstranitelných rizik (§ 102 odst. 2). Zaměstnavatel je povinen vyhledávat rizika, zjišťovat jejich příčiny a zdroje a přijímat opatření k jejich odstranění (§ 102 odst. 3). Nelze-li rizika odstranit, je zaměstnavatel povinen je vyhodnotit a přijmout opatření k omezení jejich působení tak, aby ohrožení bezpečnosti a zdraví zaměstnanců bylo minimalizováno (§ 102 odst. 4). [17]

Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, zabraňuje neoprávněnému nakládání s osobními údaji a jejich zneužití. V rozsahu působnosti tohoto zákona stanoví, kdo je oprávněn ověřovat osobní údaje a jak s nimi musí nakládat, aby nemohly být zneužity. [23]

Zákon o Policii České republiky

Zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, stanovuje činnosti a úkoly policie, upravuje její organizaci a řízení, povinnosti, oprávnění a prostředky policisty. Upravuje použití donucovacích prostředků v zájmu ochrany bezpečnosti osob, své vlastní a majetku a ochrany veřejného pořádku, proti osobě, která je ohrožuje (§ 38) a použití zbraně k odvrácení nebezpečného útoku, který ohrožuje střežený nebo chráněný objekt nebo stanoviště, po marné výzvě, aby bylo upuštěno od útoku (§ 39). [26]

2.2 Technické normy

Organizace věnující se ve světě tvorbě norem v oblasti biometrie sou především:

- Mezinárodní organizace pro standardizaci ISO (ISO - International Organization for Standardization) a Mezinárodní elektrotechnická komise (IEC - International Electrotechnical Commission)
- Mezinárodní komise pro standardizaci informačních technologií M1 (INCITS - International Committee for Information Technology Standards)
- Společná technická komise JTC1 (JTC 1 - Joint Technical Committee) a Subkomise SC 37 (SC 37 - Subcommittee)
- Organizace pro rozvoj strukturovaných informačních standardů OASIS (OASIS - Organization for the Advancement of Structured Information Standards)
- Americká národní instituce pro standardy ANSI (ANSI - American National Standards Institute)
- Německý normalizační ústav DIN (DIN - Deutsches Institut für Normung);
  např.: DIN NI-AHGB & NI-37

Vzájemná subordinace a spolupráce při tvorbě celosvětově platných norem se řídí dle diagramu (viz Příloha č.1). Biometrické normy specifikují především: formáty při výměně biometrických dat, rozhraní aplikačních programů a profilů, definice a výpočet výkonnosti systémů, přístupy k testovaní výkonnosti a požadavky na hlášení výsledků testování.

České normy v souladu s požadavky Evropské unie zabývající se bezpečností objektů:
ČSN EN 50 131-x: Požadavky na EZS (Elektrické zabezpečovací systémy)
Norma se zabývá všeobecnými požadavky na EZS, čidla, ústředny, signalizační zařízení, napájecí zdroje atd.
ČSN EN 50 132-x: Požadavky na CCTV sledovací systémy
Norma se zabývá systémovými požadavky, požadavky na černobílé a barevné kamery, objektivy, příslušenství, monitory, záznamová zařízení, přenos videosignálu atd.
ČSN EN 50 133-x: Systémy kontroly vstupů pro použití v bezpečnostních aplikacích
Norma se zabývá požadavky na systém, komponenty, vyhodnocovací zařízení, komunikaci.
ČSN EN 50 134-x: Systémy přivolání pomoci
Norma se zabývá systémovými požadavky, aktivačními zařízeními, propojením a komunikací, napájení atd.
ČSN EN 54-x: Elektrická požární signalizace (EPS)
Norma se zabývá požadavky na ústředny, sirénami, napájením, jednotlivými druhy hlásičů, systémovými požadavky, hlásiči a přenosovými zařízeními atd.
ČSN EN 74 7731: Dveře odolnější proti vloupání
ČSN P ENV 162x: Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Požadavky a klasifikace, zkušební metody pro stanovení odolnosti při statickém zatížení; zkušební metody pro stanovení odolnosti při dynamickém zatížení; zkušební metoda pro stanovení odolnosti proti manuálním pokusům o násilné vniknutí.

Soubor právních předpisů a technických norem stanovuje základní pravidla, podmínky a doporučení, podle kterých se následně zabezpečení objektu řídí. Vhodně a správně definované právní normy napomáhají projektantům bezpečnostních opatření v práci, stejně tak jako budování systému technických norem nebo alespoň schvalování již existujících zahraničních norem.

3 Biometrie a základní pojmy

Biometrie (biometric) je vědní obor zabývající se studií a zkoumáním živých organismů (bio-), především člověka, a měřením (-metric) jeho biologických (anatomických a fyziologických) vlastností a také jeho chováním, tzn. behaviorálních charakteristik. V zahraniční je pojem biometric již přímo vykládán jako proces automatizované metody rozpoznávání jedince založený na měřitelnosti biologických a behaviorálních vlastností (dle NSTC - Nation Science and Technology Council - Národní rada pro vědu a technologii USA, Výboru pro vnitrostátní a národní bezpečnost). [13]

Rozpoznávání lidí pomocí biologických charakteristik je metoda užívaná odpradávna, lidé se rozpoznávají pomocí vzhledu tváře nebo jsou známy otisky dlaní v jeskyních jako jakýsi podpis autora (některé z nich jsou až 30 000 let staré). S rozvojem počítačových technologií na konci 60.let se začalo i biometrické rozpoznávání člověka stávat automatizovaným. [13]

V problematice biometrie je nutné správně rozumět základním pojmům, jelikož mají původ v anglickém jazyce a do češtiny bývají občas nesprávně překládány.

Recognition (rozpoznávání) je druhový termín, který nutně nemusí znamenat identifikaci ani verifikaci. Jedná se o rozpoznávání člověka použitím vhodné tělesné vlastnosti.

Verification (ověření nebo verifikace) označuje proces, při kterém se biometrický systém pokouší potvrdit totožnost jedince, který se s ní prokazuje, srovnáním sejmutého vzorku s již dříve zapsaným (tzv. šablonou neboli template). Jedná se o tzv. princip one-to-one (1:1).

Identification identifikace je proces, kdy se biometrické systém pokouší určit totožnost neznámého jedince. Biometrická informace je sejmuta a porovnávána se všemi uloženými vzorky (šablonami). Princip je znám jako one-to-many (1:M).

Authentication (autentifikace, autentizace nebo legalizace) je pojem, který lze sloučit s termínem rozpoznávání. Ovšem na konci procesu v tomto případě získá uživatel určitý status, např. oprávněný/neoprávněný atd.

3.1 Metody autentizace

Všechny systémy pracující s automatizovaným přístupem jsou závislé především na principu, kterým je přístup zabezpečen. V základě existují tři mechanismy pojetí: použití hesla, předmětu nebo biometrického prvku.

3.1.1 Autentizace heslem

Použití hesla jako prostředku pro přístup do systému je stále nejpoužívanějším principem zabezpečení. Velký podíl na tom má i jeho globální použití v osobních počítačích, počítačových sítí, emailových účtech, u SIM karet mobilních telefonů a u platebních karet. Bezpečnost je v tomto případě zajištěna tím, že si omezený počet uživatelů (nejlépe jeden) pamatuje určitou posloupnost znaků, kterou mu umožní přístup do chráněné oblasti. Výhody hesel jsou snadný způsob realizace a nízká cena pořízení. Velká řada nevýhod ovšem použití hesel omezuje na systémy s nízkým stupněm zabezpečení. Mezi největší nevýhody patří možnost dekódování speciálními programy, zapomenutí nebo vysledování neoprávněnou. Bezpečnost lze v omezené míře zvýšit používáním vhodných zásad, jako je složení z malých i velkých písmen nebo speciálních znaků, dostatečná délka, neobvyklost slova nebo fráze a nesouvislost s osobou vlastníka. Zároveň musí být měněno v pravidelných intervalech, nesmí být nikde poznamenáváno a musí být distribuováno zabezpečeným způsobem. [9]

3.1.2 Autentizace předmětem

Bezpečnost tohoto principu je zaručena vlastnictvím speciálního předmětu - tokenu, který je pro přístup do systému vyžadován. Token je jedinečný předmět, co možná nejhůře kopírovatelný, vybavený informací nutnou pro autentizační protokol, čímž se ověří identita uživatele. Výhodou a zároveň nevýhodou tokenu je jeho přenositelnost, proto by měl být token vždy používán jen v kombinaci s heslem anebo jako nositel biometrického vzorku uživatele. [9]

V praxi používanými tokeny jsou:

- tokeny pouze s pamětí (magnetické, elektronické nebo optické karty) jako obdoba mechanického klíče
- tokeny s heslem - vyžadují zadání hesla zároveň s použitím, např. platební karty

- logické tokeny - dokáží zpracovávat jednoduché podněty, např. vydej klíč/cyklickou sekvenci klíčů
- inteligentní token - mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, mohou umět šifrovat a generovat náhodná čísla

3.1.3 Biometrická autentizace

Biometrika využívá jedinečných tělesných znaků pro identifikaci osoby. Výhodou tohoto typu autentizace je, že není nutné pamatovat si několika místné kombinace hesel či neustále s sebou nosit snadno zcizitelný token. Biometrická autentizace je rychlou a pohodlnou a velice přesnou metodou, která je navíc levným řešením, vzhledem ke svým neexistujícím pozdějším nákladům. Její hlavní výhodou je skutečnost, že biometrické charakteristické znaky zůstávají během života relativně neměnné a nelze je ukrást či zapomenout.

Podstatou všech biometrických systémů je automatizované snímání biometrických charakteristik a jejich následné porovnávání s údaji předem sejmutými. Cílem v oblasti bezpečnosti je vytvoření komplexních systémů založených na kombinaci měření více charakteristik. Tím se bezpečnost těchto systémů mnohonásobně zvýší. Současné biometrické systémy pracují s různými charakteristickými znaky člověka jako jsou: otisk prstu, geometrie tváře, duhovka oka, sítnice oka, geometrie ruky, geometrie prstů, struktura žil na zápěstí, tvar ucha, složky lidského hlasu, lidský pach, DNA, dynamika podpisu a dynamika psaní na klávesnici.

Výhody biometrické autentizace jsou především:

- vysoký stupeň spolehlivosti: osvědčené technologie lze jen obtížně oklamat
- nulové provozní náklady: žádná režie spojená s procesem autentizace
- rychlost
- praktičnost: není co ztrácet ani přenášet
- zřejmost: výsledek je jednoznačný a okamžitý
- efektivnost: přímé datové propojení s databází a počítači
- cena: příznivá ve vztahu k bezpečnosti a v poměru cena/výkon, neexistující dodatečné náklady

Porovnání autentizačních metod

Hesla je možné použít pouze pro nejnižší stupně zabezpečení. Lze se jich relativně snadno zmocnit a jsou přenositelné. Tokeny jsou vhodné pro vyšší stupně zabezpečení, také se jich jde snadno zmocnit a jsou přenositelné. Kombinace tokenu a hesla lze použít pro poměrně vysoký stupeň zabezpečení. Kombinace je značně odolná při odcizení nebo ztrátě tokenu, avšak opět může selhat lidský činitel a může dojít k vyzrazení hesla a zapůjčení tokenu. Jsou přenositelné. Biometrické znaky člověka se dají použít pro nejvyšší stupeň zabezpečení. Nelze je ztratit ani předat, jsou nepřenositelné.

Souhrnně lze konstatovat , že každý typ zabezpečení je možno podrobit útokům. Tyto hrozby snižujeme použitím jednotlivých autentizačních metod ve vzájemných kombinací. Použití biometrické specifické vlastnosti člověka v automatických systémech řízení a kontroly vstupů však představuje v současnosti nezastupitelný prostředek pro dosažená nejvyššího stupně zabezpečení objektu.

4 Elektronické biometrické rozpoznávací systémy

Využití elektronických biometrických rozpoznávacích systému v praxi má široké uplatnění, ať už se jedná o soukromou nebo forenzní sféru. Ve srovnání s manuálními metodami má takový systém řadu výhod vyjmenovaných dříve v kapitole 3.1.3. Ve forenzní sféře je světově nejznámější a nejvíce používaný systém AFIS (Automated Fingerprint Identification System - Automatický systém pro identifikaci dle otisku prstu), vyvinutý vládou USA ve spolupráci s FBI (Federal Bureau of Investigation - Národní úřad pro vyšetřování) a NSTC. Tento systém je instalován i v České republice v Praze pod názvem AFIS200, který byl dodán společností De Lat Rue Printrac, jeho pořízení stálo přes 100 miliónů Kč. Podobné systémy pracující na jiných principech než je otisk prstu lze najít v mnoha státech světa. Velký rozmach nastává s automatickou identifikací dle DNA a systémů pracujících na průběžném vyhodnocování geometrie tváře osob v davu (použitelný na nádražích, letištích, rušných náměstí atd.) Velký vliv na jejich implementaci v každém státě má i postoj odpovědných osob. Dále je nutno poznamenat rozvoj biometrické identifikace u cestovních pasů a při bankovních peněžních transakcí. [20]

Jak je ovšem zřejmé z ceny pořízení takovýchto systémů, je zcela nepřijatelné uvažovat o jejich implementaci v komerční sféře. Abychom dosáhli redukce ceny je nutné přehodnotit princip celého systému. Hlavní rozdíl u soukromého systému je především v mnohem menší databázi jak biometrických vzorků tak i samotných osob. Taktéž není např. u otisků prstů nutné ukládat otisky všech deseti prstů, jak to mu bývá v kriminalistické sféře, ale pouze jen jednoho. Proto si systém vystačí z mnohem menší kapacitou paměti a hlavně operačním výkonem, který jde ruku v ruce s cenou celého systému.

4.1 Biometrické systémy řízení a kontroly vstupů

Systémy kontroly a řízení vstupů v bezpečnostních aplikacích (ACS - Access Control Systems) hlídají vstup do chráněných prostor a vstup do těchto prostor umožňují pouze uživateli, který se prokazuje nějakou metodou autentizace. ACS systémy spadají pod normu ČSN EN 50133. Verifikace značí ověřovací proces v systému ACS, který vždy vyžaduje přihlášení uživatele do systému, kde je poté provedeno porovnání neskenovaného záznamu se záznamem v databázi. Je důležité omezit počet možných přihlašovacích pokusů, než bude uživatel systémem definitivně odmítnut jako nepovolaná osoba. Pro daný počet přihlašovacích pokusů je nutné vzít v úvahu úroveň zabezpečení systému. Čím menší počet pokusů zvolíme tím s větší pravděpodobností vyvoláme několik falešných poplachů kvůli neprovedené identifikaci oprávněného uživatele. Na druhou stranu je ale nutné zvolit takový počet pokusů, aby neoprávněný uživatel neměl čas získat dostatek informací o systému, které by mu později pomohly systém prolomit. [9]

U vysoce zabezpečených systémů by měly být výsledky verifikace pro pozdější zpracování ukládány. Nabízí se tři možnosti: přímo do zařízení (do hlavní jednotky snímače) nebo do vzdáleného počítače nebo přímo do tokenu pokud je použit. Ukládání přímo do snímače je nevýhodné vzhledem k omezené paměti jednotky a ke snadnějšímu přístupu k uloženým datům pro narušitele. Při plné paměti by starší záznamy byli pravděpodobně přemazávány novějšími. Při ukládání do vzdáleného počítače není proces omezen velikostí paměti, ale existuje určité nebezpečí průniku do systému zvnějšku, čili je nutné tuto komunikaci i samotnou databázi dále zabezpečit. Třetí způsob, ukládání dat do tokenu, je nevýhodný z hlediska nutnosti složitější elektroniky a rozhraní pro token, tedy z hlediska ceny řešení a stupně zabezpečení. [11]

4.2 Princip biometrických systémů řízení a kontroly vstupů

Předpokladem pro provedení biometrické autentifikace je sejmutí a zápis biometrické vlastnosti osoby, která je dále uložena jako osobní referenční šablona buď decentralizovaně na čip ID karty nebo počítače, nebo centrálně do datové paměti systému nebo aplikace. Je nutné provádět snímání a zápis opatrně, jelikož kvalita pořízeného obrazu má zásadní vliv na proces autentifikace. Je zřejmé, že proces snímání musí být prováděn v důvěryhodném prostředí.

Většina biometrických systémů pracuje s následujícím postupem: [3]

- Pořízení datového souboru (obraz, zvuk, atd.), který obsahuje biometrickou vlastnost, která z něj jde vyextrahovat použitím vhodného snímače (senzoru).
- Prověření kvality dat: pokud jejich kvalita nevyhovuje jsou okamžitě odmítnuta nebo je uživateli poskytnuta vhodná rada pro zvýšení kvality sejmuté biometrické vlastnosti (např. upozornění na směr snímání, polohu části těla atd.)
- Vyextrahování požadované biometrické veličiny z datového souboru a vytvoření šablony vzorku
- Zápis: uložení šablony jako referenční šablony do archívu referenčních šablon systému či aplikace (dle definování místa ukládání)
- Ověřování: porovnání aktuální (vyžadované) šablony s referenční šablonou užitím algoritmu pro určení shody a vygenerování hodnoty (skóre), která je rozhodná pro determinování stupně shody
- Výsledek ověřování: pokud skóre shody překročí předdefinovanou hranici, tak je přístup umožněn, v opačném případě je žádost odmítnuta.

Biometrické informace používané pro identifikaci

Kritéria pro výběr biologické nebo behaviorální vlastnosti člověka určené pro jeho další identifikaci jsou determinována co nejširším a nejefektivnějším způsobem užití. Takto vhodná vlastnost člověka musí splňovat:

- jedinečnost: vlastnost musí být co možná nejvíc výjimečná, tzn. že se shodná vlastnost nesmí objevit u dvou lidí zároveň
- univerzálnost: vlastnost musí být měřitelná u co možná největší množiny lidí
- trvalost: vlastnost se nesmí měnit v čase

- měřitelnost: vlastnosti musí být měřitelné shodnými technickými zařízeními
- uživatelská přijatelnost: vlastnost musí být snadno a pohodlně měřitelná

Nejlépe prozkoumané a nejvíce rozšířené biometrické vlastnosti používané pro identifikační účely jsou uvedeny níže spolu se stručným popisem toho, co se měří:

- otisk prstu (struktura papilárních linií a jejich detailů)
- dynamika podpisu (rozdíly v tlaku a rychlosti psaní)
- geometrie tváře (vzdálenosti specifických částí - oči, nos, ústa…)
- duhovka oka (obrazový vzorec duhovky)
- sítnice oka (struktura žil na očním pozadí)
- geometrie ruky (rozměry dlaně a prstů)
- struktura žil na zápěstí (struktura žil)
- tvar ucha (rozměry viditelné části ucha)
- hlas (tón a zabarvení hlasu)
- DNA (řetězec deoxyribonukleové kyseliny)
- pach (chemické složení)
- psaní na klávesnici (rytmus úderů do klávesnice PC)

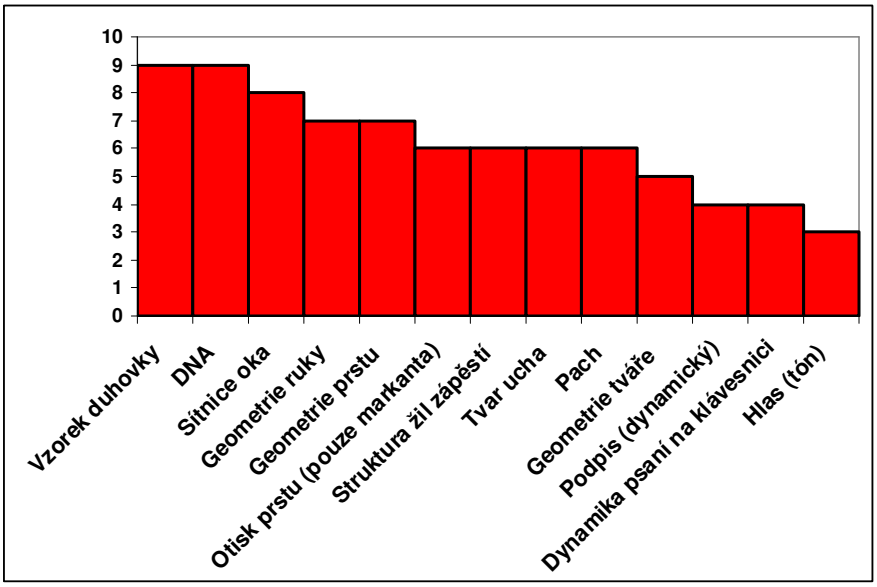
Způsoby kterými biometrické vlastnosti člověka vznikají jsou v základě tři:

- skrze genetický vývoj: uplatňuje se vliv dědičnosti (DNA) - genotypické
- skrze náhodné varianty vzniku v časném stádiu vývoje embrya - randotypické
- skrze učení a výchovu: chování jedince - behaviorální

Je dokázáno, že všechny tři faktory přispívají k vývoji biometrické vlastnosti, ačkoliv každý v jiné míře. **Příloha č.2/1** přehledně hodnotí relativní důležitost jednotlivých faktorů (1 znamená zanedbatelný vliv, 3 významný vliv). [3]

Jak již bylo zmíněno je jedním z nejdůležitější požadavků na biometrickou vlastnost její stálost v čase, aby nemohlo dojít k její kompromitaci se stárnutím člověka. Důvodů proč se vlastnost může změnit je několik. Vliv růstu živé tkáně, opotřebení, biologické stárnutí, špína a nečistoty, zranění a následné hojící procesy a nespecifikované vlivy. Biometrické vlastnosti, které jsou nejméně ovlivněné těmito možnostmi jsou nejvíce upřednostňovány.

Stupeň stálosti v čase je znázorněna v následujícím grafu č.1 (10 znamená nejvyšší stálost v čase, 0 nejnižší). [3]



Graf 1: Stálost biometrické vlastnosti v čase

Z poměrně široké škály možností využití jedinečné vlastnosti člověka je nutné se v praxi umět správně rozhodnout, který princip zvolit. Abychom byli schopní jednotlivé principy srovnávat musíme si stanovit kritéria. Je zřejmé, že budeme referovat takovou biometrickou vlastnost, která bude pro uživatele i správce komfortní, navíc bude dostatečně přesná, dostupná pro co identifikování co možná největšího okruhu lidí a zároveň bude i cenově přijatelná. **Příloha č.2/2** nám přehledně popisuje výhody a nevýhody jednotlivých biometrických znaků. [3]

Je těžké definovat optimální biometrickou metodu. V poměru cena a přesnost vychází nejlépe otisk prstu. Duhovka oka má vysoké hodnocení ve všech kategoriích v případě, že cena nehraje roli vychází duhovka oka nejlépe. DNA ztrácí body v komfortu snímání a také v přesnosti, protože jednovaječná dvojčata mají shodnou DNA.

4.3 Měření výkonnosti biometrických systémů

Efektivnost biometrických rozpoznávacích systémů lze měřit mnoha statistickými koeficienty. Charakteristickými výkonnostními mírami jsou koeficient nesprávného přijetí, koeficient nesprávného odmítnutí, koeficient vyrovnané chyby, doba zápisu etalonu a doba

ověření. Takových koeficientů existuje ovšem celá řada v závislosti na hloubce zkoumání problému. [3]

False Acceptance Rate (FAR) - Koeficient nesprávného přijetí udává pravděpodobnost toho, že neoprávněná osoba je přijata jako oprávněná. Jelikož nesprávné přijetí může často vést ke vzniku škody, FAR je především koeficient udávající míru bezpečnosti. Označuje se jako chyba II. druhu.

False Rejection Rate (FRR) - Koeficient nesprávného odmítnutí udává pravděpodobnost toho, že oprávněný uživatel je systémem odmítnutý. FRR je především koeficient udávající komfort, protože nesprávné odmítnutí je pro uživatele nepříjemné. Označuje se jako chyba I. druhu.

Failure to Enroll Rate (FTE nebo FER) - Koeficient selhání přihlášení. Udává poměr osob, u kterých selhal proces přihlášení do systému. Jedná se o pohyblivou veličinu, která má vztah nejen k osobě, ale i ke konkrétní biometrické vlastnosti, která se snímá. Lze poté určit i tzv. osobní FER udávající vztah konkrétní osoby a jejích biometrických vlastností k procesu snímání. V případě, že byla uživateli správně sejmuta biometrická vlastnost, avšak systém ho chybně odmítl i po mnoha identifikačních/verifikačních pokusech, mluvíme o tzv. koeficientu selhání přístupu FTA (Failure To Acquire).

Abychom získali spolehlivé statistické údaje, je nutno provést velké množství pokusů o sejmutí biometrické vlastnosti. Pravděpodobnost neúspěchu sejmutí vlastnosti konkrétní osoby se vypočte podle vzorce 1.1.

$$FER(n) = \frac{počočneúspesnych\ pokusů\ o\ zápis\ u\ 1\ osoby\ (nebo\ 1\ vlastnosti)\ n}{celkovy\ pocet\ pokusů\ o\ zápis\ u\ 1\ osoby\ (nebo\ 1\ vlastnosti)\ n} \quad (1.1)$$

Čím více pokusů provedeme, tím lepší hodnoty nám vycházejí. Celkové FER pro N účastníků (uživatelů) je definován jako průměr z FER(n) podle vzorce 1.2.

$$FER = \frac{1}{N} \cdot \sum_{n=1}^{N} FER(n) \quad (1.2)$$

Čím více uživatelů se bude započítávat, tím přesnější hodnoty nám budou vycházet.

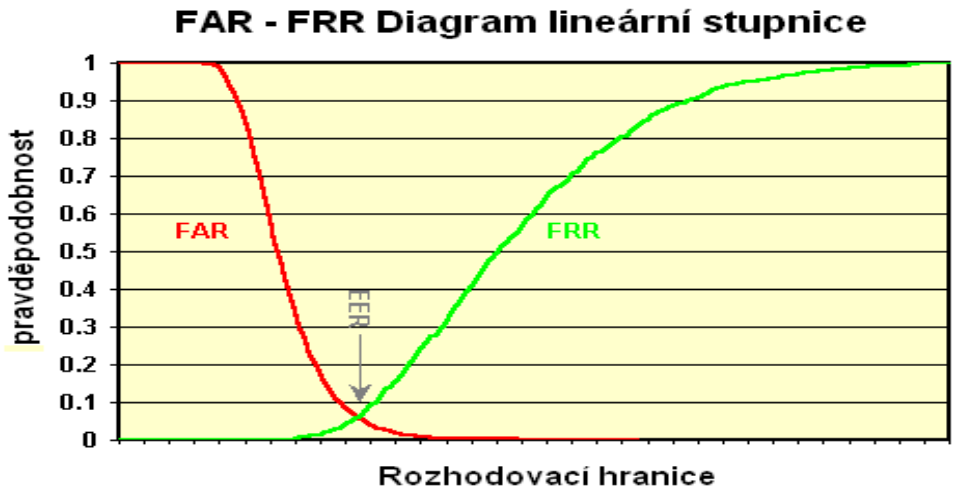
False Identification Rate (FIR) - Koeficient nesprávné identifikace udává pravděpodobnost, že při procesu identifikace je biometrická veličina (vlastnost) nesprávně

přiřazena k některému referenčnímu vzorku. Přesná definice závisí na principu, kterým se přiřazuje pořízený vzorek k referenčnímu, jelikož se často stává, že po srovnávacím procesu vyhovuje více než jeden referenční vzorek, tzn. překračuje rozhodovací práh.

False Match rate (FMR) - Koeficient nesprávné shody udává poměr neoprávněných osob, které jsou chybně rozpoznány jako akreditované během srovnávacího procesu. Porovnáme-li ho z koeficientem FAR liší se v tom, že na rozdíl od FAR se do FMR nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. Znamená to tedy, že koeficienty FAR a FRR jsou více závislé na způsobu používání biometrického zařízení.

False Non-Match Rate (FNMR) - Koeficient nesprávné neshody udává poměr toho, že oprávněné osoby jsou chybně nerozpoznány během srovnávacího procesu. V porovnání s FRR se liší v tom, že se nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu.

Důležitým pojmem při měření efektivnosti (výkonnosti) biometrických systémů je tzv. křížový koeficient, udávající s jakou pravděpodobností při jakém nastavení hranice rozhodování nastane jev FAR a FFR současně (tzn. FAR=FFR). Křížový koeficient EER (Equal error rate) je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR. Je-li FAR koeficientem bezpečnosti a FRR koeficientem komfortu, je zřejmé, že ve chvíli kdy jsou v rovnováze je v rovnováze i celkové nastavení systému. Následující diagram (viz Graf 2) průniku pravděpodobnostních distribučních funkcí FAR - FRR názorně ukazuje jak se v závislosti na nastavené hranici rozhodování projeví celková pravděpodobnost, že mohou nastat obě chyby stejně pravděpodobně. [3]



Graf 2: Distribuční pravděpodobnostní funkce FAR -FRR

Použití v soukromé praxi

V soukromé sféře naleznou automatické biometrické systémy pro rozpoznávání uplatnění v mnoha oblastech:

Ochrana počítačů a dat

- přístupy k uživatelským účtům a souborům
- přístupy do serverů a sítí
- aplikační software
- komerční využití internetu

Zajištění komfortu

- náhrada průkazů
- stravovací systémy, kasina
- uživatelské nastavení (PC, automobily atd.) bezhotovostní platební transakce

Přístupové systémy

- zajištění zabezpečení vstupu do objektu nebo chráněných prostor
- obytné objekty, sklady, elektrárny, letiště, výpočetní střediska, trezory

Docházkové systémy

- evidence docházky a pohybu osob v objektu či areálu (státní i soukromé instituce)
- automatické ovládání EZS, aktuální přítomnost zaměstnanců, podklady pro mzdy apod.

4.4 Biometrické technologie

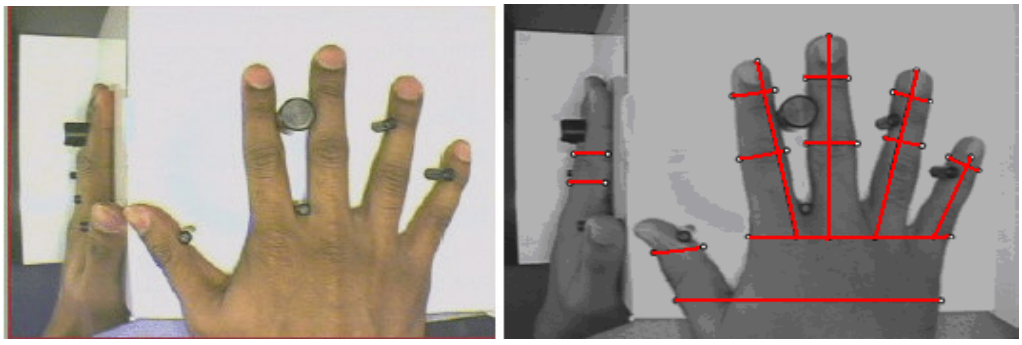
Od žádné biometrické technologie nelze očekávat, že splní podmínky pro jakékoliv identifikační aplikace. Bylo zkoumáno mnoho možností biometrické identifikace, každá z nich má své silné stránky a své limitace. V této kapitole je popsán souhrn existujících a rychle se rozvíjejících biometrických technologií.

4.4.1 Geometrie ruky

Systémy rozpoznávající geometrii ruky jsou nestarším implementovaným biometrický principem. Vyvinul a nechal si jej patentovat David Sidlauskas v roce 1985 a hned v příštím roce byli již systémy rozpoznávající geometrii ruky komerčně dostupné. V roce 1996 byly tyto systémy použity pro identifikaci na Olympijských hrách v Atlantě, kde zajišťovaly

bezpečnost vstupu do olympijské vesnice. Jelikož ale není geometrie ruky příliš unikátní biometrickou vlastností, je její aplikace v bezpečnostní sféře omezena právě stupněm bezpečnosti, kterého chceme dosáhnout. [13]

Zařízení pro rozeznávání geometrie ruky využívají jednoduchého principu měření a 3 dimensionálního snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka umístěné na podložce s pěti polohovými kolíky (viz Obrázek 1) pomocí CCD kamery.



Obrázek 1: Ruka se zrcadly snímaná CCD kamerou a příklad měření vzdáleností

Na obrazu ruky lze najít přes 31 000 polohových bodů a provést 90 různých měření vzdáleností. Vybrané měřené informace lze se ukládají do 9 bitového souboru, což činí tyto systémy velice výhodné z hlediska nízkého požadavku na paměť systému. Biometrické systémy založené na verifikaci geometrie ruky jsou používány v různorodých aplikacích docházkových systémů a přístupových systémech, kde jsou poměrně velmi rozšířené. [13]

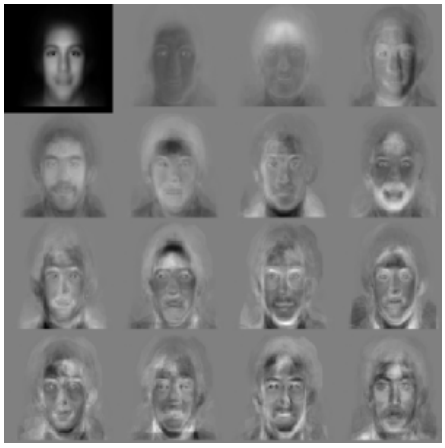
V USA je systém normalizován ANSI INCITS 396-2005. Celosvětově použitelní norma ISO/IEC CD 19794-10 - Part 10 Geometrie ruky, je stále ve stádiu návrhu a nebyla ještě schválena.

FRR: <0.1%; FAR: 0.1%; čas verifikace: 1 až 2 sekundy; míra spolehlivosti: střední

4.4.2 Geometrie tváře

Existují dva odlišné přístupy k rozpoznávání geometrie tváře: geometrický (založený na rysech tváře) a fotometrický (založený na vzhledu obrazu tváře). Tři nejlépe prozkoumané a studované algoritmy rozpoznávání tváře jsou: Analýza hlavních částí (PCA - Principal Components Analysis), Lineární diskriminační analýza (LDA - Linear Discriminant Analysis), Elastický srovnávací diagram (EBGM - Elastic bunch graph matching). [13]

PCA využívá vektorů tváře odvozených s kovarianční matice pravděpodobnostní distribuční funkce k vytvoření šablony vhodné pro srovnávání. Každá tvář lze rozdělit na tzv. eigenfaces (vzory tváří - matice jasových úrovní) a poté jde opět složit (viz. Obrázek 2). Každá eigenface je reprezentována pouze číslem, takže se namísto obrázku ukládá pouze číslo. [13]

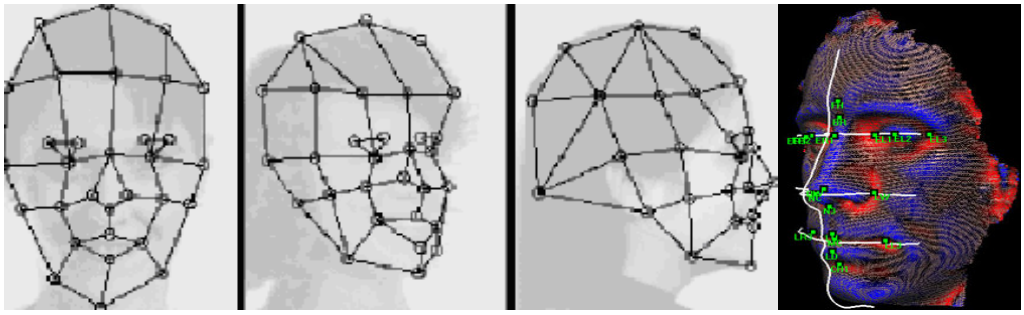


Obrázek 2: Standardní eigenfaces používané pro rozložení obrazu

LDA je metoda, kdy se třídí pořízené obrazy tváří do skupin. Cílem je maximalizovat rozdíly mezi jednotlivými skupinami a minimalizovat rozdíly v každé skupině, každý blok snímků reprezentuje jednu třídu (viz Obrázek 3). [13]

Obrázek 3: Příklad šesti tříd užitím LDA

EBGM byla vyvinuta, jelikož předešlé metody nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, pozice hlavy anebo výraz tváře (úsměv, zamračení). Na obličeji se definuji uzlové body, které se poté propojí a tím definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje (viz. Obrázek 4). Samotné rozpoznávání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat. Problémem je přesnost lokalizace orientačních bodů na tváři, řešením může být kombinace s PCA nebo LDA metodou. [13]



Obrázek 4: Síť vytvořená elastickým mapováním a obraz zpracovaný počítačem

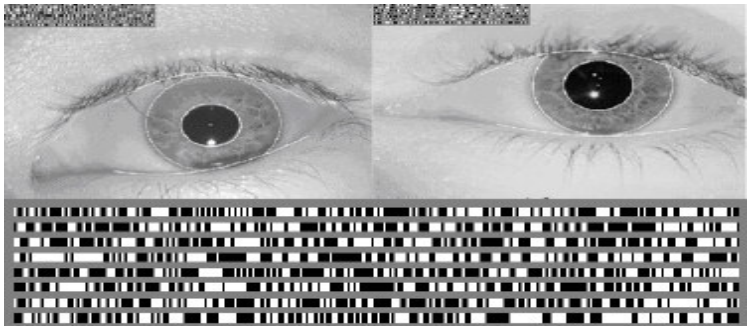
Identifikace osob dle geometrie tváře je dnes velice moderním a expandujícím principem. Dochází k jejími nasazování na letištích, nádražích, rušných ulicích a náměstích a všeobecně na místech, kde by se mohli pohybovat hledaní lidé apod.

FRR: <1%; FAR: 0,1%; čas verifikace: 3 sekundy; míra spolehlivost: střední

4.4.3 Duhovka oka

Automatické biometrické systémy pro rozpoznávání duhovky lidského oka jsou relativně nové vyvinuté. První patent je datován k roku 1994 a vyvinul ho Úřad pro jadernou bezpečnost USA včele s Dr. Johnem Daugmanem. Duhovka je sval uvnitř oka, který reguluje velikost čočky (tedy zaostření oka) na základě intenzity světla dopadajícího na oko. Duhovka je barevná část oka, jejíž zabarvení odpovídá množství meletoninového pigmentu uvnitř svaloviny. Ačkoliv je zabarvení i struktura duhovky geneticky závislá, její vzorkování není. Duhovka se vyvíjí během prenatálního růstu plodu a její vzorkování je náhodné, tudíž jedinečné pro každého člověka i dvojčata, dokonce i jeden člověk má každou duhovku jinou, což činí tyto systémy nejpřesnějšími ze všech. [13]

Snímání duhovky vyžaduje velice kvalitní digitální kameru a infračervené osvětlení oka. Během snímání se duhovka mapuje do fázorových diagramů, které obsahují informaci o orientaci, četnosti a pozici specifických plošek. Tyto informace pak slouží k vytvoření duhovkové mapy (viz Obrázek 5) a šablony pro identifikaci.



Obrázek 5: Lokalizování duhovky a její piktografické znázornění

Při verifikačním procesu se porovnává žadatelova mapa duhovky s tou referenční pomocí testu statistické nezávislosti. Pokud je pouze méně než jedna třetina dat odlišná, test statistické nezávislosti selhal, což znamená že vzorky jsou ze stejné duhovky.

FRR: 0,00066%; FAR: 0,00078%; čas verifikace: 2 sekundy; míra spolehlivosti: vysoká

4.4.4 Sítnice oka

Pro rozpoznávání osoby dle její sítnice oka se používá obraz struktury cév na pozadí lidského oka v okolí slepé skvrny. Sítnice je světlo-citlivý povrch na zadní straně oka a je složena z velkého množství nervových buněk. Pro získání obrazu se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém (dnes se již používá pouze jedna infračervená LED dioda, což snižuje riziko nebezpečného ozáření oka oproti používání systému několika LED diod). Neskenovaný obraz je poté převeden do podoby 40 bitového čísla. Verifikace sítnice je velice přesnou metodou identifikace. Její používání vyžaduje od uživatele, aby se díval do přesně vymezeného prostoru, což může být pro některé osoby nepříjemné a někdy až nemožné, pokud používají brýle. Z těchto důvodů nemá tato metoda rozšířenou oblast používání a její použití se shrnuje na oblasti vůbec nejvyššího stupně zabezpečení. [13]

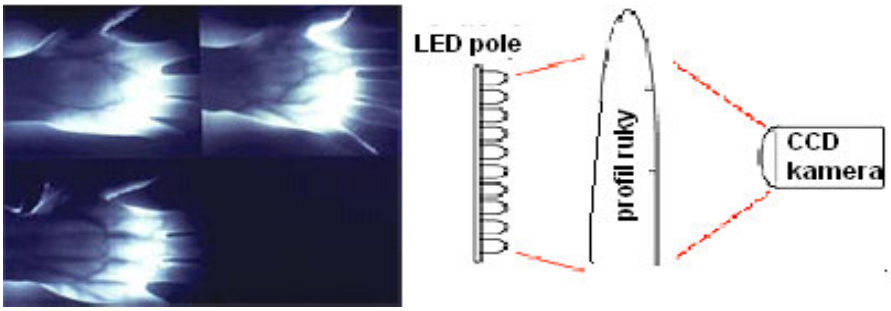
FRR: 0,4%; FAR: 0,001%; čas verifikace: 1,5 až 4 sekundy; míra spolehlivosti: vysoká

4.4.5 Struktura žil na zápěstí

Jedná se o jednu z nejnovějších metod rozpoznávání jedince (první komerčně dostupné systémy jsou datovány až k roku 2000). Využívá se k ní jedinečné vlastnosti struktury cév člověka na jeho zápěstí (popř. jen prstu), která se nemění ani během stáří Tato

technologie se vyznačuje obtížností falšování (síť cév je obtížné napodobit, jelikož je uvnitř ruky a není tedy viditelná pro napodobení; navíc některé principy přímo vyžadují, aby byla ruka živá, tedy aby v ní tekla teplá krev). Výhodou je také bezkontaktní princip (uživatel se nemusí dotýkat povrchu snímače, což zvyšuje hygienu a pravděpodobnost správného přijmutí uživatele). Pro uplatnění této technologie existuje mnoho různých použití (např. v Japonsku jsou systémy rozmístěny na univerzitách, nemocnicích a pokladních automatech). Aplikace musí mít zajištěnu ID verifikaci, vysokou fyzickou bezpečnost kontroly přístupů, vysokou bezpečnost datových sítí a kontrolu přístupu do pokladních systémů. Další nespornou výhodou je možnost verifikace i identifikace (lze použít pro systémy 1:1, kdy se používá ID karet nebo jiných tokenů, anebo systémů 1:N, kdy je pořízený vzorek porovnáván s celou databází šablon).

Snímání probíhá následovně: blízký zdroj (pole LED diody) prosvítí ruku a na základě různé absorpce (odrazu) záření krevních cév a ostatních tkání se vytvoří obraz (viz Obrázek 6) pomocí snímací CCD kamery (charge-coupled device - zařízení s nábojovou vazbou). Obraz je dále digitalizován a zpracováván za cílem vyextrahování sítě cév. Ukládají se důležité vlastnosti jako: body a úhly větvení cév a tloušťka cév.

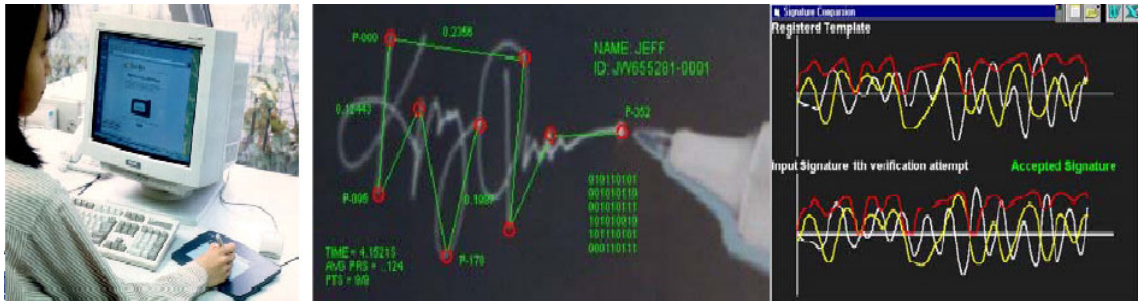


Obrázek 6: Obraz světelné propustnosti ruky a princip snímání

4.4.6 Dynamika podpisu

Tato metoda je datována k roku 1977 a využívá jedinečnosti kombinace anatomických a behaviorálních vlastností člověka, které se projeví když se podepisuje. Zařízení na dynamický podpis se často mylně zaměňují s pojmy jako je elektronický podpis (šifrovaný klíč) nebo se zařízeními na snímaní podpisu jako obrazu. Z ručního podpisu lze tak elektronicky zjistit tah, tvar a tlak při psaní, což lze použít pro verifikaci osoby. Jednotlivé

druhy zařízení se liší dle výrobce způsobem užití a jeho významem, ale mají shodnou vlastnost použití technologií citlivých na dotek, tedy PDA záznamníků nebo digitalizačních tabulí. Většina těchto zařízení využívá dynamických vlastností podpisu, ačkoliv existují i kombinace se statickými a geometrickými vlastnostmi podpisu. Základními dynamickými vlastnostmi jsou rychlost, akcelerace, časování, tlak a směr tahu, které jsou zaznamenávány v trojrozměrném souřadnicovém systému (viz Obrázek 7). Osy ‚x' a ‚y' slouží k určení rychlosti a směru tahu, souřadnice ‚z' určuje tlak na podložku. Na rozdíl od statického obrazu podpisu, který může být naučen a napodobován, je nemožné se dynamiku podpisu pouze z obrázku naučit. Výhodou je i snadné integrování zařízení do již existujících systémů (stačí PDA a vhodný SW). Naopak nevýhodou je, že tyto systémy jsou schopné zvládat pouze verifikační principy. [13]



Obrázek 7: Princip dynamického podpisu; uživatel - měření - SW srovnání

4.4.7 Dynamika chůze

Stejně jako otisk prstu nebo duhovka oka je i pohyb člověka jedinečný a svým způsobem neoklamatelný a v relativně širokém časovém období neměnný. České kriminalistice a jejímu výzkumu patří přední místo ve světě ve vývoji identifikace člověka podle stylu chůze, odborně „pohybu po dvou nohách" neboli bipedální lokomoce. Velký podíl na rozvoji této metody má i rozmach záznamové a snímací techniky. Průkopníkem tohoto odvětví identifikace je prorektor pro vědu a výzkum Policejní akademie v Praze Prof. PhDr. Jiří Straus DrSc., který se zkoumání lidské chůze věnuje přes 25 let.

Stejně jako při identifikaci podle ručního písma je rozlišovacím znakem jedinců různý dynamický stereotyp, u písma se jedná o stereotyp ruky a chůze celého pohybu těla. Tato metoda má obrovský význam při identifikování pachatelů loupežných přepadení, jimž je zcela zbytečné jakákoliv maskování nebo převleky. Další význam tato metoda nabývá

při současném prudkém rozvoji nasazování průmyslových kamer na nejrůznější rušná místa (letiště, náměstí, nádraží, multifunkční komplexy atd.). Její uplatnění je tedy pouze ve forenzní sféře, kde však dosud stále neexistuje databáze srovnávacích materiálů.

Celá metoda pracuje na základě porovnávání křivek drah, které opisují určité body na lidském těle, tedy hlavně jeho těžiště. Jelikož je každý člověk jedinečný svým pohybovým svalově kosterním systémem a svým dynamickým stereotypem, jsou i křivky uvažovaných bodů unikátní a vhodné pro srovnávání a 1:1 identifikaci. Způsob vytváření těchto křivek viz **Příloha č.3/3**.

4.4.8 Otisk prstu

Identifikace na základě otisku prstu je jednou z nejznámějších a nejvíce publikovaných biometrických metod. Otisk prstu se používá pro identifikaci už celé století, a to hlavně pro svou vlastnost jedinečnosti a stálosti v čase. Navíc se musela tato identifikace s rozvojem počítačové techniky stát plně automatizovanou, aby si zajistila místo v dnešní době. Identifikace dle otisku prstu je s oblibou používaná především pro relativní jednoduchost získání srovnávacího vzorku, pro vysoké procento použitelné populace (nelze identifikovat pouze jedince, kteří přišli o obě ruce i nohy, což je málo pravděpodobné), dále pro četnost zdrojů o ze kterých lze získat vzorek (10 prstů) a také protože jde již o zavedenou metodu s velkou databází u policie a s uplatněním v právní sféře a imigrační problematice. [13]

Používání otisku prstu (přesněji obrazců papilárních linií na vnější straně prstů rukou, nohou a dlaní) jako metody pro identifikaci se začala používat už na konci 19. století, kdy Sir Francis Galton nalezl a definoval některé charakteristické body na prstu, které mohou sloužit k identifikaci člověka. Tyto „Galtonovi body“ položily základ vědnímu zkoumání otisku prstu, který byl rozvíjen po celé století. [14]

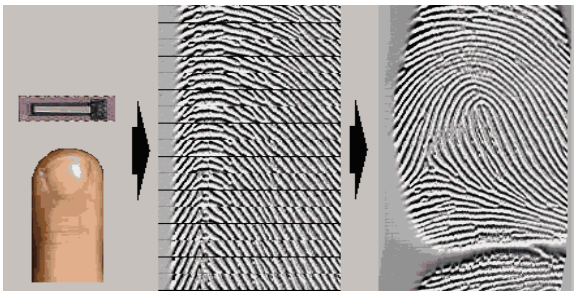
Metody zachycení otisku prstů

Otisk získaný pomocí inkoustu a papíru - Klasická metoda (rolled finger). Tato metoda se používá pouze ve forenzní sféře, policií při vyšetřování. Používá se inkoustu a papíru. Prst se po papíře roluje, aby se získal otisk celého prstu (prakticky od nehtu po nehet)

s co možná nejvíce použitelnými markantami a aby se tím zvýšila i rychlost rozpoznání otisku. [3]

Statické snímání - Jedná se o nejběžnější používanou metodu snímání otisku prstu. Uživatel přitiskne svůj prst na senzor bez jakéhokoliv pohybování s ním. (existují desítky různých fyzikálních principů snímání, které jsou vysvětleny dále). Výhodou této metody je nesporně jednoduché ovládání (stačí pouze přiložit prst). Na druhou stranu je zde řada nevýhod: přehnanou silou tlačení prstu může uživatel rozlomit snímací čočku (obzvlášť je-li doba snímání delší, uživatel znervózní a přitlačí více), přiložení prstu a jeho současné pootočení vede k deformaci pokožky a celého otisku, senzor se lehce zašpiní (nehygieničnost) a na senzoru můžou zůstat latentní otisky. [14]

Snímání šablonováním - Uživatel přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů (viz Obrázek 8). Používá-li se křemíkový snímač, pohybuje se i cena v oblasti křemíkových součástek. Redukovat cenu lze právě využitím šablonovaného snímání, tím že snímač bude mít tvar úzkého pruhu. Celková cena pro pořízení otisku prstu je poté výrazně nižší. Výhody šablonovaného snímání jsou: snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor; na snímači nezůstávají skryté (latentní) staré otisky; uživatel nemá pocit ‚zanechaného' otisku prstu a snímání je rychlé. Nevýhodou je, že obsluha takového zařízení není intuitivní a uživatel se musí naučit určitý postup. [14]



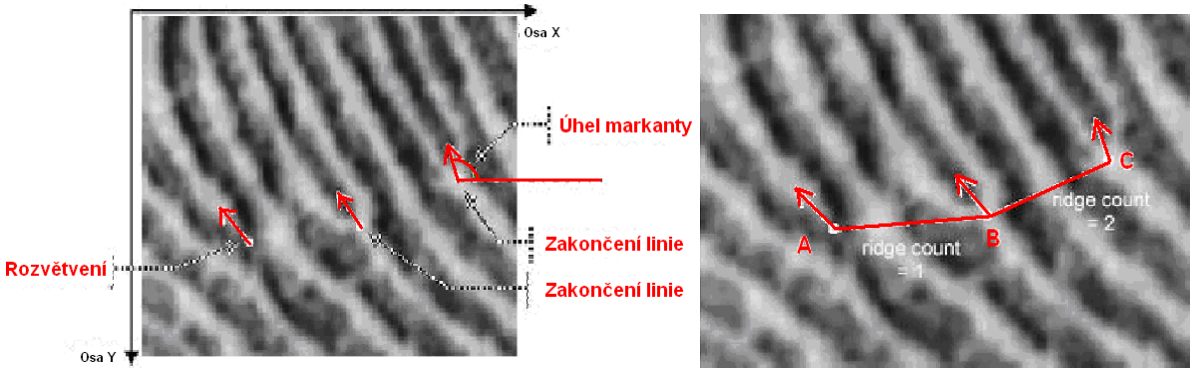
Obrázek 8: Postup zachycení obrazu otisku prstu šablonováním

Používané algoritmy u snímačů otisku prstu - Srovnávací metody.

Většina algoritmů využívá existence markant, specifických bodů jako je zakončení linie, rozvětvení linie, bod (ostrov), jezero, výběžek (osten) nebo zkřížení, což jsou detaily třech hlavních vzorů (seskupení papilárních linií). Jedná se o smyčky, víry a oblouky (loop, whorl, arch) viz **Příloha č.3/1**.

Některé algoritmy ukládají pro pozdější srovnávání pouze pozice (s=[x;y]) a směr (úhel Θ) markant, což vede k redukci dat nutných pro zápis (viz Obrázek 9a). [3, 11, 14]

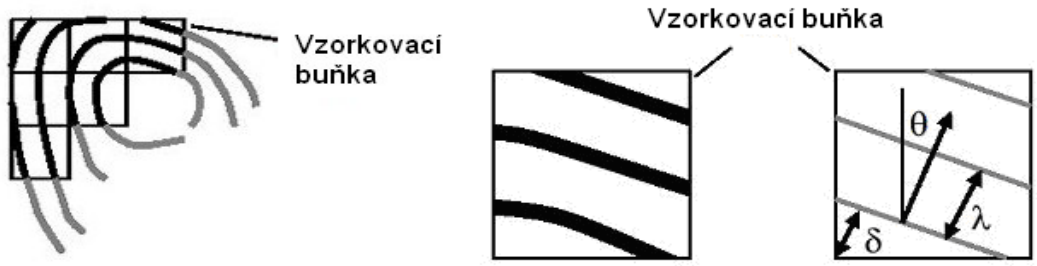
Jiné algoritmy namísto vzdálenosti znaku vypočítané z pozice, sčítají počet vyvýšených rýh mezi dvěmi konkrétními body, zpravidla markantami (viz Obrázek 9b).



Obrázek 9: a) Příklady vzorkování markant **b) Příklad algoritmu sčítajícího vyvýšeniny**

Často používaný algoritmus vytváření tzv.markantografu pracuje na vytvoření obrazce spojnicemi mezi nalezenými markantami. Postup je následovný: obraz originálu otisku prstu je podroben filtru orientace markant, následné počítačové binarizaci dat, zeslabení linií, nalezení markant a vytvoření markantografu (viz **Příloha č.3/2**).

Pro jiný srovnávací algoritmus je základní vzhled rýh. Samotný otisk prstu je rozdělen do malých sektorů, z nichž se vyextrahují a uloží: směr rýh, jejich vzájemný odstup a fáze (viz. Obrázek 10). Velmi často používají algoritmy, které jsou kombinací několika metod.



Obrázek 10: Vzorkovací buňky a zjišťování sklonu linie Θ, odstupů linií λ a odstupů od okraje buňky δ

U komerčního použití je práh citlivosti (hranice počtu shodných markant) volitelná dle bezpečnostního požadavku. Ve forenzní sféře je nutno splnit podmínku daného státu (v ČR se jedná o minimální počet 10 shodných markant, v USA 8, v Rusku 7, v EU 10-17).

FRR: <1,0%; FAR: 0,0001% - 0,00001% dle technologie; čas verifikace: 0,2 - 1 sekunda; míra spolehlivosti: vysoká

Určení pravděpodobnosti, že dva různé otisky prstů budou shodné:

Podle vlastních výzkumů společnosti IBM/Pankanti je pravděpodobnost odhadována na $6 \cdot 10^{-8}$. Existuje ovšem velké množství způsobů výpočtů pro odhad pravděpodobnosti. V následující tabulce č.1 M, R definují snímanou oblast a N počet markant. [3]

Tabulka č.1: Výpočty pravděpodobnosti shody otisku prstu

Autor	P (otisk prstu)	N=36; R=24; M=72	N=12; R=8; M=72
Galton (1892)	$\frac{1}{16}\times\frac{1}{256}\times\left(\frac{1}{2}\right)^{R}$	$1{,}45\times10^{-11}$	$9{,}54\times10^{-7}$
Pearson (1930)	$\frac{1}{16}\times\frac{1}{256}\times\left(\frac{1}{36}\right)^{R}$	$1{,}09\times10^{-41}$	$8{,}65\times10^{-17}$
Henry (1900)	$\left(\frac{1}{4}\right)^{N+2}$	$1{,}32\times10^{-23}$	$3{,}72\times10^{-9}$
Gupta (1968)	$\frac{1}{10}\times\frac{1}{10}\times\left(\frac{1}{10}\right)^{N}$	$1{,}00\times10^{-38}$	$1{,}00\times10^{-14}$
Roxburgh (1933)	$\frac{1}{1000}\times\left(\frac{1{,}5}{10\times2{,}412}\right)^{N}$	$3{,}75\times10^{-47}$	$3{,}35\times10^{-18}$
Stoney (1985)	$\frac{N}{5}\times0{,}6\times\left(0{,}5\times10^{-3}\right)^{N-1}$	$1{,}20\times10^{-80}$	$3{,}50\times10^{-26}$

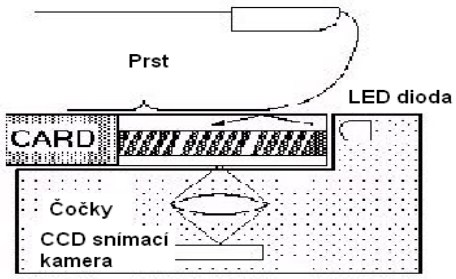
Snímače otisků prstů

Existují desítky metod snímání otisku prstu využívajíc nejrůznější fyzikální principy. Vědci se neustále snaží o nalézání nových a nových metod, a avšak ty nejjednodušší a nejsnadnější jsou již objeveny a používány. Jedná se především o:

1. Optické senzory
   - Na základě odrazu (reflexní)
   - Reflexní se skládáním obrazu
   - Bezdotykový odraz
   - Transmisní
   - TFT optické
2. Elektro-optické snímače
3. Kapacitní snímače
   - Křemíkové čipy a kapacitní snímač
   - Kapacitní snímač a TFT

4. Tlakové snímače
   - Vodivá membrána na silikonu
   - Vodivá membrána na TFT
   - Dotekové mikro-elektro-mechanické spínače
5. Rádiové snímače
6. Teplotní senzory
7. Ultrazvukové snímače
8. Fotonové krystaly
9. Snímače povrchové impedance

Optické senzory na základě odrazu (reflexní) - Optické senzory patří mezi nejstarší technologii snímání otisku prstu. Hlavní princip spočívá v přidržení prstu nad skleněnou podsvětlenou vrstvou, světlo se odráží od prstu a prochází do CCD snímače, který zachycuje vizuální obraz otisku (viz. Obrázek 11). Nevýhoda tohoto typu je, že je poměrně náchylný k chybám a tím k opakovanému snímání (špinavý prst nebo skenovací ploška vede ke špatnému obrazu, z čehož vyplývají vyšší nároky na údržbu). [11, 14]



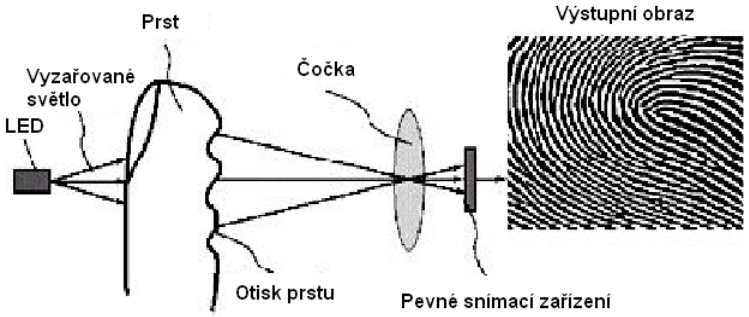
Obrázek 11: Princip snímání reflexními optickými senzory

Optické senzory na základě odrazu (reflexní) se skládáním obrazu - Princip je stejný jako u předchozího snímače, ale výsledný obraz není snímán staticky ale šablonováním. Používají se reflexní rolovací senzory, kdy je jedno-dimenzionální snímací zařízení spolu se zdrojem světla a optickými čočkami umístěno v průhledné rolovací tubě, po které prst klouže. [11]

Optické bezkontaktní snímače - TST (Touchless Technology - bezkontaktní technologie) nepotřebuje optický hranol pro přímé snímání obrazu prstu. Světelné paprsky vysílané z LED diod se odrážejí podrůznými úhly od papilárních linií prstu do optické čočky. Signál zpracovává CMOS čip. [3]

Transmisní optické snímače - Princip (viz Obrázek 12) je založen na snímání světelných paprsků procházejících prstem ruky, který je z vrchní části prosvěcován všesměrovým zdrojem světla (většinou klasická infračervená LED dioda). Obraz otisku prstu

je poté zpracován stejně jako u předchozích principů systémem čoček a snímacím zařízením. Dle druhu výrobce se jedná buď o standardní CCD (Charged Coupled Device) kameru (společnost Mitsubishi), CMOS (Complementary Metal Oxid Semiconductor) kameru (společnosti NEC, Delsy) anebo i s využitím polymerického organického fotodetektoru vyvinutým společností NanoIdent. [3]



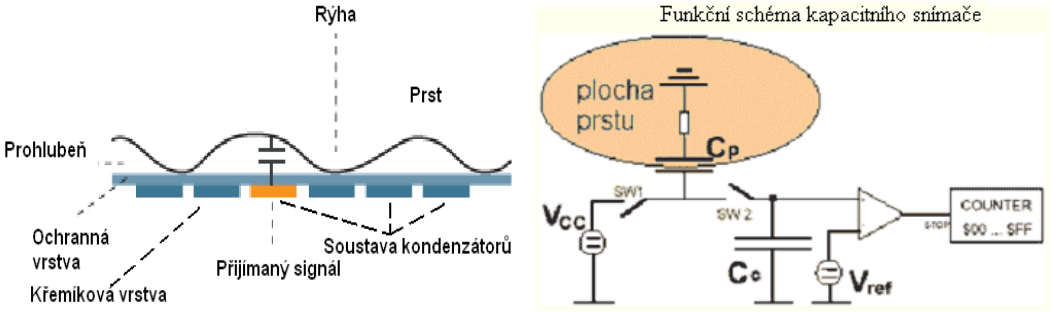
Obrázek 12: Princip transmisních snímačů otisku prstu

TFT optické snímače - U tohoto typu snímačů dochází k nahrazení klasického snímacího zařízení, tedy určitého typu kamery (CMOS nebo CCD), TFT displejem (TFT - Thin Film Transistor). [3]

Elektro-optické snímače - Princip snímání je založen na faktu, že některé polymerní materiály jsou schopné emitovat světelné záření pokud se nabudí vhodným napětím. Pokud takovýto materiál přímo propojíme se snímacím zařízením (CMOS kamerou) lze získat obraz otisku prstu tím, že polymerní materiál emituje světlo jen v místech kde se ho přiložený prst dotýká, tzn. ve styčných bodech papilárních linií. Zařízení tohoto typu vyrábí společnost Ethentica a korejská společnost TesTech. [3]

Kapacitní snímače otisku prstu - Jedná se o nejrozšířenější princip (viz Obrázek 13) snímání otisků, který je založen na měření kapacity mezi kůží prstu a aktivními pixely. Velikost měřeného elektrického pole se mění mezi rýhami a prohlubněmi struktury papilárních linií jako příčina změny dielektrika mezi jednou deskou kondenzátoru (pixelem) a druhou deskou kondenzátoru (prstem). Dielektrikem je tedy buď vzduchová vrstva (prohlubeň-pixel) nebo pokožka (rýha-pixel). Citlivá snímací plocha je tvořena deseti tisíci kondenzátory strukturovaných do sítě. Senzory využívající kapacitní princip jdou zdaleka nejpřesnějšími typy, jejich výhodou může být i velmi malý rozměr senzoru (zpravidla kolem 4 cm^2). Snímacím zařízením může být u této metody opět buď CMOS kamera (Fujitsu,

Hitachi, Symwave), TFT displej (Mitsubishi, Alps Electric) nebo progresivní metoda silikonových čipů (NTT Laboratories, Shigematsu). [3, 8, 11, 13, 14]



Obrázek 13: Kapacitní princip snímání otisku prstu

Rádiové snímače otisku prstu - Aktivní kapacitní snímače - Princip je založen na měření síly rádiového signálu, který je vysílán do prstu vysílačem nízkého RF (Radio frequency) signálu a snímán maticí miniaturních antén, které tvoří styčnou plochu z prstem. Síla signálu se mění v závislosti odporu či vodivosti spojení, tedy na vzdálenosti mezi kůží a anténní soustavou tvořenou pixely, znamená to tedy, že rádiový signál bude jiný v místě kde se prst přímo dotýká senzoru (rýhy papilárních linií) a v místě kde se ho nedotýká (prohlubně papilárních linií). [3, 14]

Tlakové snímače otisku prstu - Piezoelektrické materiály, které jsou schopny snímat změnu tlaku existují již dlouho, ale problémem byla jejich citlivosti pro detaily papilárních linií. Jedním z řešením je umístit vodivostní membránu (tvořenou maticí piezoelektrických tlakových senzorů) na CMOS kameru se silikonovým čipem (společnost Opsis). Jiná metoda umístí membránu na TFT podložku (společnost Sanyo, Fidellica, Alps Electric). Jedna z nejmodernějších metod využívá maticového systému mikro mechanických spínačů o velikosti pouhých 50µm, které tvoří síť spínací v místech kde se prst dotýká svými prohlubněmi papilárních linií. [3, 14]

Teplotní snímače otisku prstu - Tepelné snímání pracuje na principu měření nepatrných rozdílů teploty mezi pokožkou prstu a vzduchu, který vyplňuje prostor mezi jejími papilárními liniemi. Neměří se absolutní velikost teploty, ale právě rozdíl mezi tepelnou energií pokožky předané senzoru v momentě, kdy se dotkne jeho snímací části. Ta je vyrobena z křemíkového čipu pokrytého pyro-elektrickým materiálem, neboli materiálem který je citlivý na změny teploty. Na křemíku je nanesen v podobě přiléhajících pixelů.

Teplotní diference se díky pyro-elektrickému materiálu převede na elektrický náboj, který je poté, díky samotným vlastnostem této látky, zesílen a předán na spodní křemíkový čip (který je také uspořádán do pixelů). Ten pak převede hodnoty elektrických signálů na samotný obraz v několika stupních šedi. [3, 11, 14]

Ultrazvukové senzory - Ultrazvukové senzory narozdíl od optických, které měří odražené světlo, měří odraženou zvukovou vlnu. Technologie funguje na podobných principech jako sonar. Jejich výhodou je, že ultrazvuk snadno pronikne i nečistotami, které by znehodnotili obraz zachycený pomocí optického snímače.

Požadavky na senzory

- Vyhovující celkové rozměry - Tento požadavek je snadno splnitelný u systémů určených pro přístup do místnosti, budov atd. Pro přístup do počítačů, notebooků apod. je již potřeba miniaturizace zásadní.
- Dostatečně velká snímací plocha - Dostatečná snímací plocha je nutná pro záznam dostatečného počtu identifikačních znaků (markant), nebo plochy obrazu. Existuje malá skupina lidí, která má extrémně málo markant nebo má část markant vyhlazených prací.
- Dostatečné rozlišení - Požadavek na rozlišení je dán především použitým algoritmem na rozpoznání, požadavky na spolehlivost a nastavením chyb prvního a druhého druhu pro systém. Kvalitní obraz by neměl mít zkreslení, měl by mít dostatečný kontrast a obsahovat pokud možno co nejširší škálu rozsahu šedé barvy.
- Opakovatelnost dosažené kvality obrazu otisku prstu - Pro dosažení dobrých výsledků při autentizaci z hlediska hodnot chyby prvního a druhého druhu je důležitá opakovatelnost kvality obrazu otisku. Posun obrazu otisku vzhledem k etalonu a jeho natočení musí být při pokusu o autentizaci minimální.
- Dostatečná ochrana vůči napodobeninám - Snímač sám o sobě nezabezpečuje dostatečnou ochranu vůči napodobeninám. Jedná se o slabé místo celého systému. Některé testy s napodobeninami vykazují dokonce lepší poměr FAR a FRR než původní lidské biometrie. Řešením je dodatečná ochrana pomocí kamer nebo fyzické přítomnosti ostrahy.
- Uživatelská přívětivost - Uživatelská přívětivost je základním požadavkem ve směru k uživateli systému a ergonomii snímače.

– Odolnost vůči mechanickému poškození - Většina snímačů je konstruována pro připojení k počítači a neprošla zkouškami na odolnost vůči mechanickému poškození ani zkouškami ve ztížených klimatických podmínkách, což je chyba.

– Spolehlivost snímačů otisků prstu - Spolehlivost je zjišťována především testy na chybu prvního a druhého druhu. Řada výrobců udává ovšem hodnoty, které nejsou dosažitelné ani teoreticky.

– Životnost snímačů - Jedná se o konstrukční prvky snímačů, u nichž je z podstaty omezena životnost. Jsou to především materiály, které chrání snímací plochu vůči poškození.

– Cena snímače - Cena snímače je velmi variabilní v závislosti na řadě faktorů. Přesto je z výše uváděného rozboru zřejmé, že zřejmě nejdražší budou kvalitní optoelektronické snímače.

Při realizaci konkrétního návrhu zabezpečení pomocí ACS je nutno zvážit všechny aspekty a vytvořit vhodný kompromis s požadavky zadavatele projektu. Šíře v současnosti nabízeného sortimentu dává však projektantům bezpečnostních opatření dostatečně velký prostor pro naplnění těchto cílů.

5 Návrh biometrického zabezpečení systému řízení vstupu do administrativního objektu

V této kapitole je popsána problematika spojená se zabezpečením vstupních prostor do imaginárního objektu státní správy, a sice objektu spadajícím pod Ministerstvo vnitra České republiky (dále jen MV ČR), kde si zadavatel projektu určil, že je vyžadována třída identifikace 3 a třída přístupu B dle ČSN EN 50133-1. Dále dle ČSN EN 50131-1 je vyžadována třída bezpečnosti 2. Dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, je vyžadována kategorie objektu V (vyhrazené). V závislosti na těchto podmínkách a výsledků analýzy rizik bude řešeno optimální zabezpečení.

5.1 Popis chráněného objektu

Objektem ochrany je vstupní malá hala dvoupodlažní nevýrobní administrativní budovy, která má kancelářský charakter. Vstup do objektu je možný pouze hlavním vchodem, který vede do vstupní haly. Z prostor haly ústí ven pouze vchodové dveře a ventilační šachta. Stavební konstrukce objektu je železobetonová zděná o tloušťkách nosné konstrukce 500 mm a tloušťce příček 200 mm. Znázornění haly viz **Příloha č.4/1**.

V objektu je zaměstnáno celkem 33 zaměstnanců, administrativní pracovníci jsou rozděleny do dvou směn po 15 lidech (ranní směna od 8:00 do 16:00 a odpolední směna od 16:00 do 24:00). Tři pracovníků ostrahy jsou zároveň jako obsluha dispečinku v prostorách vrátnice rozděleni do tří směn (ranní směna od 8:00 do 16:00, odpolední směna od 16:00 do 24:00 a noční směna od 24:00 do 8:00). Jedná se o externí zaměstnance soukromé bezpečnostní služby.

5.2 Stávající bezpečnostní opatření vstupních prostor

Technická bezpečnostní opatření - Vchod je zabezpečen klasickým dřevěným dveřním křídlem, vybetonované zárubně jsou osazeny dvěma závěsy. Uzamykací mechanismus je kovový jednobodový zámek s mosaznou 5 stavítkovou cylindrickou vložkou FAB. Certifikace dle ČSN P ENV 1627 je 2. bezpečnostní třída.

Oddělovací vchod pro chráněné prostory je zabezpečen nízkým otočným turniketem se třemi segmenty karuselu. Autentizace předmětem probíhá na základě vlastnictví autorizované ID karty.

Instalována EPS (elektrická požární signalizace). Na ústřednu EPS jsou napojeny opticko-kouřové hlásiče, požární klapky a tísňová tlačítka. Jejich rozmístění je řešeno v rámci požadavků schvalovacího řízení stavby a bylo potvrzeno kolaudačním rozhodnutím. Instalováno analogové PIR čidlo připojené na zastaralý typ ústředny EZS.

Fyzická ochrana a režimová opatření - Fyzická ochrana je realizována 24 hodin denně vždy jedním pracovníkem ostrahy, který má statické pracoviště v prostorách vrátnice. Pracovník dohlíží na bezproblémový pohyb ve vstupní hale, hlídá pokusy o neoprávněné vniknutí do chráněných prostor, řeší kontrolní opatření při vstupu a výstupu do objektu

a problémy s identifikací uživatelů. Na vyžádání má právo kontrolovat osobní věci v důsledku snahy o neoprávněné vynášení předmětů a informací.

Stávající režimová opatření jsou řešena především bezpečnostní prověrkou způsobilosti všech zaměstnanců podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů a změn. Dále řeší vlastníka klíčů od hlavního vchodu. Tím je pouze pracovník ostrahy a vedoucí každé směny. Klíč pracovníka ostrahy musí být vždy umístěn v prostorech vrátnic a nesmí se vynášet ven. V případě nepřítomnosti vedoucího směny řeší právě on odemknutí hlavních dveří. Dále je řešeno střídání směn ostrahy, kdy pracovník smí opustit stanoviště až ve chvíli, kdy je fyzicky přítomna další směna.

5.3 Ohrožení chráněného objektu administrativní budovy

V uvažovaném objektu se nachází movitý majetek a finanční prostředky, včetně osobního majetku zaměstnanců. Dále se zde pracuje s utajovanými informacemi kategorie V (vyhrazené).

Popis hrozeb při vniknutí do chráněných prostor:

- neoprávněné nakládání s utajovanými informacemi vnějšími neoprávněnými narušiteli (šíření, kopírování, vynášení z objektu, poskytování druhé osobě, znehodnocování, úpravy atd.)
- vniknutí do chráněných prostor neoprávněným narušitelem a jejich následná ztráta důvěryhodnosti (možnost sabotáže, teroristického útoku, únosu, popř. jiného trestného činu)
- nezákonné nakládání s osobním majetkem a majetkem státu (odcizení, znehodnocování atd.)
- vnitřní hrozby - zneužití pravomoci nakládat s utajovanými informacemi oprávněnými osobami

Bylo provedeno modelování rizika pomocí FTA (Fault Tree Analysis) pro vybranou hrozbu únik utajované informace, viz **Příloha č.5/1**.

5.4 Analýza rizik chráněného objektu

Bude provedena analýza možností poruch a jejich následků FMEA (Failure Modes and Effects Analysis) za účelem snížení potencionálního rizika poruch. Výběrem stěžejních rizik daného systému (vstupních prostor objektu) a jejich hodnocením pomocí indexů vybereme pomocí Paretovy analýzy ty nejzávažnější a vhodnými opatřeními je budeme minimalizovat. Vypočteme míru rizika pomocí vzorce (1.3).

$$R = P \times N \times H \tag{1.3}$$

Index ‚P' určuje pravděpodobnost vzniku a existence rizika. Má 10 stupňů, ale pro potřeby analýzy použijeme pouze zkrácených 5 stupňů:

1 - nahodilá, velice nepravděpodobná

2 - spíše nepravděpodobná

3 - pravděpodobná, reálná hrozba

4 - velmi pravděpodobný vznik

5 - trvalá hrozba

Index ‚N' určuje jaké má dané riziko závažnost následků z hlediska finančního, materiálního, ohrožení zdraví osob či životního prostředí:

1 - malý delikt (úraz, škoda)

2 - větší delikt (úraz s pracovní neschopností, větší škoda)

3 - střední delikt (úraz s převozem do nemocnice, vyšší škoda)

4 - těžký delikt (těžký úraz s trvalými následky, vysoká škoda)

5 - smrt osob, velmi vysoká škoda na majetku

Index ‚H' je index odhalitelnosti rizika (události) určuje, jak rychle a jak snadno dané riziko či událost zjistíme:

1 - riziko odhalitelné v době jeho spáchání

2 - snadno odhalitelné riziko během pár minut

3 - odhalitelné riziko do jednoho dne

4 - nesnadno odhalitelné riziko (den a více)

5 - neodhalitelné riziko

Míra rizika ‚R' bude v rozmezí 0-125. Pomocí tabulky míry rizika jsme pak schopni určit do jaké kategorie riziko zařadíme:

0 - 3 Bezvýznamné riziko

4 - 10 Akceptovatelné riziko

11 - 50 Mírné riziko

51 - 100 Nežádoucí riziko

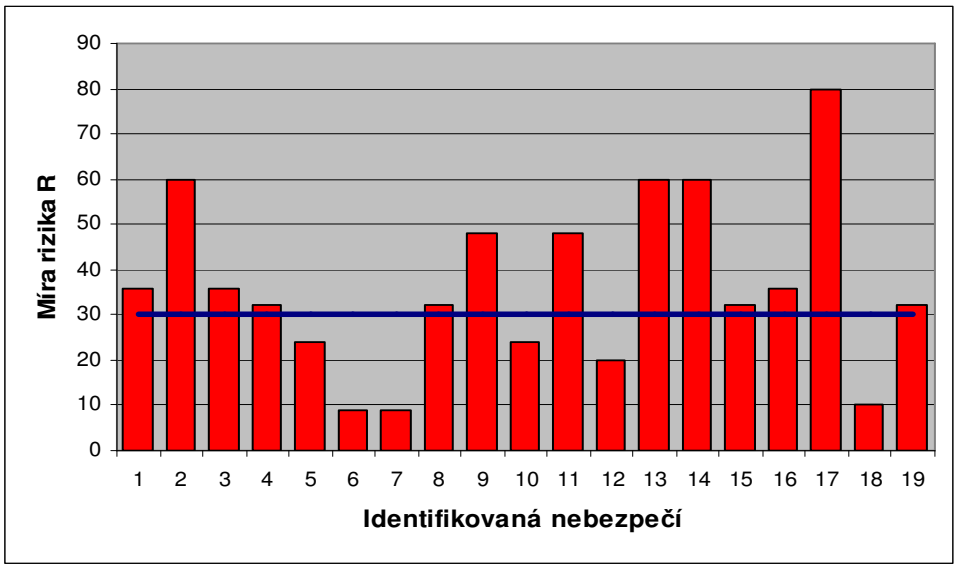
101 - 125 Nepřijatelné riziko

Jak je patrné reálnost výsledné míry rizika je závislá na toleranci analytika, jež si volí stupnici bodového ohodnocení. Pro určení zda je riziko přijatelné nebo nepřijatelné provedu Paretův diagram a Lorenzovu křivku. Vypočetl jsem sumu všech hodnot míry rizika ‚R' identifikovaných nebezpečí a vyjádřil je v procentech, poté jsem spočetl kumulativní četnost. Jednotlivá procentuální vyjádření nebezpečí jsem sčítal od nejvyšších hodnot až do celkového součtu 80%, což je stanovená hranice pro přijatelná a nepřijatelná rizika. Identifikovaná nebezpečí, která spadají do stanoveného limitu 80 % jsem vyhodnotil jako rizika nepřijatelná a pro ně jsem navrhnul další opatření. Ostatní nebezpečí jsem vyhodnotil jako přijatelné a jejich stávající opatření jsou dostačující. U každého rizika jsou uvedeny kontrolní opatření, příčiny vzniku rizik, jejich následky a podmínky jaké je nutno dodržovat, aby k nežádoucím událostem nedošlo.

Výčet identifikovaných nebezpečí a jejich míry rizik z hlediska strukturálního (jejich grafický přehled viz Graf č.3). Byla vypočtena míra tolerance R na hodnotě 32, v tom případě všechny identifikovaná nebezpečí s hodnotou 32 a vyšší budou řešena novými opatřeními ke snížení rizika (označená červeně). Nepřijatelná rizika jsou červeně zvýrazněna:

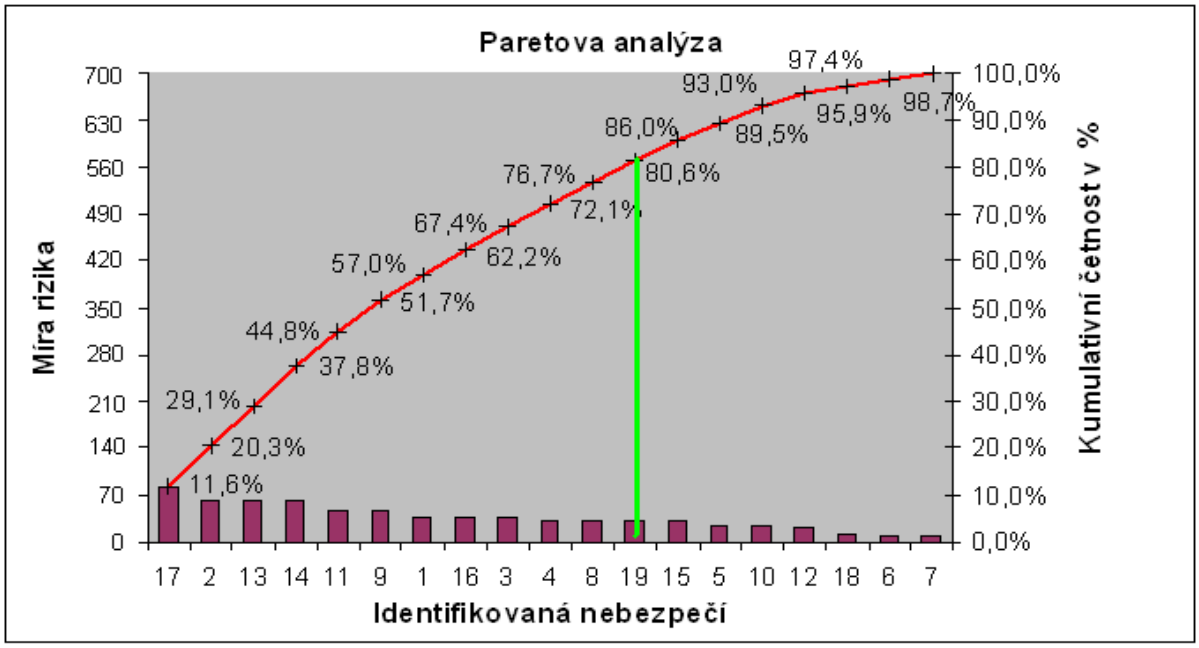
1. Neoprávněný průnik do vstupní haly R = **36**
2. Vyhmatání zámku R = 60
3. Odvrtání zámku R = **36**
4. Vypáčení dveřního křídla ze závěsů R = **32**
5. Roztažení zárubní R = 24
6. Vybourání těžkými nástroji, vozidlem R = 9
7. Překonání složitými nástroji R = 9

8. Pohyb nežádoucích osob po vstupní hale a přístup k ACS R = **32**
9. Sabotáž PIR čidla R = **48**
10. Útok na fyzickou ostrahu R = 24
11. Vniknutí do ventilační šachty R = **48**
12. Založení požáru R = 20
13. Neoprávněný vstup osob do chráněných prostor R = **60**
14. Přelezení nízkého turniketu R = **60**
15. Zneužití odcizené ID karty R = **32**
16. Sabotáž systému ACS R = **36**
17. Přístup falšováním ID karty R = **80**
18. Výpadek elektrického proudu R = 10
19. Vniknutí do systému ACS a zneužití uložených dat R = **32**



Graf č.3: Ohodnocení identifikovaný nebezpečí

Použitím Paretovy analýzy a Lorenzovi křivky kumulativních četností byl sestrojen diagram (viz Graf č.4) s použitím hodnot rizik s tabulky FMEA (viz **Příloha č.6**).



Graf č.4: Paretova analýza

Z vytvořené FMEA analýzy je zřejmé, že největší nedostatky stávajícího zabezpečení jsou především průnik přes hlavní dveře pomocí vyhmatání zámku, vniknutí do ventilační šachty, překonání nízkého turniketu a falšování identifikace uživatele u ACS, jelikož je autentizace řešena pouze vlastnictvím tokenu (ID karty) registrovaného v databázi. Nepřijatelná rizika budou v kapitole návrhu optimalizace zabezpečení prostor řešena opatřeními a snížena na přijatelnou úroveň. Je důležité si uvědomit, že riziko nelze nikdy úplně odstranit, lze pouze minimalizovat.

Pro systém kontroly a řízení vstupů Synel PrintX byla provedena analýza FTA s výpočtem rizika využitím klasické Booleovské algebry pro selhání systému ACS (viz **Příloha č.5/2**) podle vztahů 1.4, 1.5 a 1.6. Jednotlivé primární pravděpodobnosti jsou relevantní vzhledem k statistickým faktům nebo díky nim dopočítány. Celková pravděpodobnost selhání přístupového systému je $P_{faultACS} = 11 \cdot 10^{-3}$, což odpovídá jedné nesprávně provedené operaci z 90 uskutečněných.

Na chybu II. druhu FAR má majoritní vliv především $p_{template}$, který vyjadřuje selhání algoritmu při porovnávání šablony z otiskem, tvořená je z dílčích pravděpodobností p_1 (selhání procesu binarizaci dat), p_2 (50% vliv - systém nesprávně přiřadí otisk k jiné šabloně vlivem většího počtu shodných šablon) a p_3 (softwarová chyba). Při nesprávné údržbě

snímače existuje i malá šance vyhodnocení skrytého latentního otisku. Víme-li, že se FAR uvažovaného zařízení pohybuje kolem 1.10^{-3}, lze si jednotlivé pravděpodobnosti dopočítat a analyticky určit relativním vlivem na celkovou chybu.

Na chybu I. druhu FRR má více než 50% vliv selhání snímání otisku $p_{snímání}$ a to především díky p_5 (nesprávným postupem uživatele) a p_4 (mechanickým poškozením prstu nebo snímače). Ostatní vlivy jsou minoritní, víme-li že se u uvažovaného zařízení pohybuje FRR kolem $1\text{-}10^{-2}$ lze si jejich pravděpodobností analyticky určit a dopočítat.

$$P_{FAR} = p_{template}(p_1 + p_2 + p_3) + p_{latentní} = 2 \cdot 10^{-4} + 5 \cdot 10^{-4} + 2 \cdot 10^{-4} + 1 \cdot 10^{-4} = 1 \cdot 10^{-3} \quad (1.4)$$

$$P_{FRR} = p_{snímání}(p_4 + p_5) + p_{zdroj} + p_{matching}(p_6 + p_7 + p_8) = 6 \cdot 10^{-3} + 1 \cdot 10^{-3} + 3 \cdot 10^{-3} = 1 \cdot 10^{-2} \quad (1.5)$$

$$P_{faultACS} = P_{FAR} + P_{FRR} = 1 \cdot 10^{-3} + 1 \cdot 10^{-2} = 11 \cdot 10^{-3} \quad (1.6)$$

5.5 Návrh optimalizace zabezpečení chráněných prostor

Pro dosažení požadavků zabezpečení vstupních prostor do objektu a snížení rizika dle výsledků analýzy FMEA bude použita vhodná kombinace bezpečnostních opatření v podobě prvků fyzické ochrany (dále jen FO), mechanických zábran a elektronického zabezpečovacího systému.

Mechanický zábranný systém (MZS):

Mechanický zábranný systém (dále jen MZS) poskytuje ochranu svou mechanickou pevností. Doba, kterou musí pachatel vynaložit na její překonání musí být delší než je pro něj únosné. Základní úlohou MZS je tedy vytvořit pevnou hranici (překážku) definovanou určitým odporem proti destrukčnímu narušení, aby se zabránilo proniknutí pachatele do oblasti chráněného zájmu. V našem případě se MZS využijí při zabezpečení vstupních dveří do haly, vzducho-ventilační šachty a jako prostředek pro zamezení vstupu do zóny vyžadující identifikovaného uživatele v podobě turniketu. Všechny technické prostředky použité v objektu s kategorií utajení musí projít certifikací Národního bezpečnostního úřadu (dále jen NBÚ). [1, 23]

Pro zabezpečení vstupních dveří navrhuji použít:

- dveřní křídlo: bezpečnostní jednokřídlé dveře SAPELI s šestibodovými čepy, bezpečnostní třída 2 (viz **Příloha č.7/1**)
- závěsy: 3D seřiditelné viditelné závěsy Simonswerk, 3-úchytové (viz **Příloha č.7/2**)
- uzamykací mechanismus s kováním: čtyřbodový bezpečnostní rozvorový zámek MUL-T-LOCK model 235 se 6 závorami a střelkou ovládaný eurocylindrickou zámkovou vložkou s ozubeným kolem (10 zubů), bezpečnostní třída pro otvorové výplně 4 dle ČSN P ENV 1627, pro úroveň přísně tajné dle NBÚ (viz **Příloha č.7/3**)

Pro zabezpečení vzducho-ventilační šachty navrhuji použít:

- rozpěrná tyč s mechanickými spínacími kontakty s návazností na EZS ústřednu

Pro zabezpečení chráněné zóny vyžadující identifikované uživatele navrhuji použít:

- vysoký turniket se třemi segmenty karuselu: plnorozměrový turniket AUTOGARD ATF 600 ovládaný výstupním relé terminálu Synel SY-400 napojeného na čtečku otisku prstu Synel PrintX/Optic (viz **Příloha č.8/2**)

Elektronický zabezpečovací systém (EZS):

Elektronický zabezpečovací systém (dále jen EZS) se skládá z prvků monitorovacích (čidel), signalizačních (akustických či optických), přenosové cesty (datové a napájecí), ústředny a zdroje napájení (síťové a záložní - baterie, dieselagregát apod.). Úkolem EZS je především registrace a předání informace, že došlo k napadení, případně bližší specifikaci místa a předání této informace do řídícího centra k odpovědným osobám. Na ústřednu EZS může být díky široké kompatibilitě většiny zařízení napojena i průmyslová kamera (okruh CCTV) nebo systém kontroly vstupů. V našem případě budou na ústřednu EZS napojeno PIR čidlo a kamera okruhu CCTV (jejich plošné pokrytí viz **Příloha č.4/2**) pro střežení prostor haly, dále biometrické zařízení kontroly a řízení vstupu, výstupní kontakty mechanické rozpěrné tyče a tísňové tlačítko umístěné na dispečinku FO. Všechny technické prostředky použité v objektu s kategorií utajení musí projít certifikací NBÚ. [2, 23]

Pro zabezpečení prostor haly navrhuji použít:

- pasivní infračervené čidlo: duální bezdrátové PIR čidlo Jablotron s elektronickým zpracováním signálu JA-60P se záclonovou čočkou JS-7902

- průmyslovou kameru: hybridní IP CCD kamera BOSCH DINION NWC 455 s ethernetovým výstupem
- tísňové tlačítko RC-88 Jablotron

Pro kontrolu a řízení vstupů navrhuji použít:

- elektronický biometrický systém: terminál Synel SY-400/A, kapacitní čtečka otisku prstu Synel PrintX, kombinovaná klávesnice a čtečka karet Synel PRX-40. Čtečky a klávesnice jsou připojeny na terminál, který svým výstupním relé ovládá mechanismus turniketu. Data se ukládají decentralizovaně v počítači správce sítě přes rozhraní RS232. Způsob zapojení viz **Příloha č.8/1**. Technická data viz Příloha č.9.
- Při takovémto rozložení HW lze libovolně vytvořit kombinace pro 1:1 identifikaci:
    - PIN → biometrie
    - ID token → biometrie
    - ID token → PIN → biometrie

Fyzická ochrana, režimová opatření:

Fyzická ochrana je definována jako soubor činností ostrahou pověřené osoby, jejímž úkolem je zabezpečit ochranu osob a majetku, bezpečnost střežených objektů a veřejný pořádek. V našem případě bude FO realizována vlastní nepřetržitou ochranou službou v podobě šesti pracovníků ostrahy ve třech směnách na dispečinku ve vstupní hale. Úkoly pracovníka budou především: kontrolní činnost, propustková činnost (řádná obsluha systému kontroly vstupů, ohlašování neoprávněných osob a návštěv), střežení prostor na pevném stanovišti, realizace bezpečnostních opatření v prostoru vstupní haly, realizace zásahu při mimořádných událostech (narušení objektu, snaha o kompromitaci systému kontroly vstupů) a dodatečné vyrozumění míst poskytujících pomoc (návaznost na automatické hlášení EZS) pomocí tísňového tlačítka, řídícím terminálem popřípadě pevnou nebo mobilní telefonní linkou.

Režimová opatření představují administrativně organizační a věcná opatření, který by měla směřovat k bezporuchovému fungování celého bezpečnostního systému. To znamená definovat režimy vstupu a výstupu osob, vjezdu a výjezdu dopravních prostředků, vynášení utajovaných skutečností. Dále režim manipulace s klíči, identifikačními prostředky a médii, které se používají v bezpečnostním systému. [27]

Pro zabezpečení prostor navrhuji:

- vybírat pracovníky FO, kteří splňují podmínky § 6-10 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších změn
- zajistit režimová opatření dle § 24-31 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších změn
- vytvořit projekt fyzické bezpečnosti dle § 32 odst. 2 zákona č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších změn [27]
- definovat statut organizace, vytvořit organizační řád a pracovní řád organizace
- vytvořit spisový řád a definovat skartační činnost

6 Současný stav biometrických rozpoznávacích systému v České republice a ve světě

V České republice existuje v současnosti řada firem nabízejících produkty pracující na základě biometrické informace, ať už se jedná o systémy kontroly vstupů a docházky, kontroly přístupu do systémů (PC, jídelny, náhrada permanentek apod.) nebo systémy určené pro speciální účely jako je kriminalistika, policie, zdravotnictví, státní správu.

Objem výrobků i samotných firem má zejména od druhé poloviny 90.let dlouhodobě rostoucí charakter, je ovšem nutno podotknout, že drtivá většina všech společností provozuje především obchodní činnost jako zástupce nebo distributor zahraničního výrobce. Vlastní iniciativu české společnosti věnují především softwarovému vývoji aplikací pro stávající zařízení a jejich začlenění do již zaběhlých systémů. K největším distributorům biometrických systémů kontroly vstupů v České republice patří:

- CoNet (nabízí především výrobky izraelské společnosti Synel)
- DIGITUS (distributor amerických společností IR Recognition, Identix a korejské společnosti Suprema)
- GRANUS (obchodní zástupce amerických firem Identix a Recognition Systems, francouzské společnosti Sagem, švýcarské společnosti Security Biometrics a ruské společnosti Vildis)

- Moeller Elektrotechnika s.r.o. (česká pobočka německé firmy Moeller)
- FINGER-PRO s.r.o. (firma společné založená českou firmou MORONG-SLUKO s.r.o. a VS USA distribuující biometrické systémy nejrůznějších světových výrobců)
- BioFS (jako jedna z mála firem vyvíjí a vyrábí biometrické identifikační a forenzní systémy v rámci spolupráce odborníků)

Objem zařízení pracujících s biometrickou informací má v rozvinutých zemí světa mnohem širší charakter než v České republice. Důležitým aspektem je i aktivní přístup soukromých firem spolupracujících s univerzitami na dalším vývoji a výzkumu. Především Spolková republika Německo, Japonsko, Tchaj-wan a USA si zakládají na trendu kooperace s univerzitním prostředím. Samotné firmy pak vyvíjí vlastní systémy s orientací na vlastní software, avšak s mnohdy stejným technickým zázemím (především senzorů). Mezi přední výrobce snímačů do biometrických zařízení patří: Atmel, Atrua, BMF, Casio, Delsy, Doan, ElecVision, Ethentica, Fidelica, Fujitsu, Hitachi, Idex, Siemens, Melfas, Mitsumi, NEC, NanoIdent, Seiko, Sharp, Sony, Upek a Veridicon.

Přední představitelé nejrůznějších zemí světa v čele s USA, Nizozemím, Spojeným královstvím Velké Británie a Severního Irska a Spolkovou republikou Německa si uvědomují důležitost identifikace na místech s velkým počtem osob (letiště, nádraží, stadiony apod.), ať již se jedná o vyhledávání pachatelů kriminální činnosti nebo potírání nelegální imigrace, stále častějším to důvodem. V současnosti je trendem vytváření široké databáze biometrických znaků všech příchozích zahraničním turistů a delikventů. Pomoci jim v tom mají i nově vydávané cestovní pasy právě s biometrickými prvky.

Co se týče Evropské unie, byl v loňském roce 2007 vybrán poskytovatel softwaru a platformy EU-BMS (EU-Biometric Matching System; Systém biometrického rozpoznávání pro Evropskou unii), která bude centrálním komponentem kolekce programů pro identitu sloužící členským zemím, což zahrnuje přes 70 miliónů lidí Evropy. Výběrové řízení vyhrála společnost s celosvětovou působností Doan.

7 Závěr

V bakalářské práci jsem se zaměřil na problematiku biometrické identifikace a její vhodné aplikaci při zabezpečování objektu s možností snížení rizika napadení objektu a ohrožení chráněných prostor.

Úvodní část jsem věnoval existujícím právním úpravám a technickým normám, které v České republice řeší ochranu majetku. Další část práce popisuje biometrii, jako samostatnou vědu zabývající se studií jedinečných lidských znaků s rozborem autentizačních metod a jejich porovnáním. Dále popisuji problematiku elektrických biometrických systémů v procesu řízení a kontroly vstupů a v současnosti dostupné biometrické technologie. Provedl jsem modelování rizik pomocí FTA a analýzu rizik pomocí FMEA u imaginárního administrativního objektu. Na základě jejich výsledků jsem navrhnul optimální zabezpečení vstupních prostor a na základě teoretických znalostí jsem je zabezpečil kombinací prostředků technické ochrany a fyzické ochrany, čímž jsem naplnil cíle práce. Je ovšem nutné si uvědomit, že při řešení konkrétního návrhu zabezpečení se vychází především z podmínek zadavatele v kombinaci s právními předpisy a technickými normami.

Závěrem lze konstatovat, že pro zajištění kontroly vstupů do objektu je použití biometrické identifikace ideálním bezpečnostním řešením, jelikož biometrie nabízí zajímavé možnosti na poli špičkových řešení autentizace. Technologické problémy ji však omezují při jednofaktorovém nasazení u aplikací s vyšší úrovní zabezpečení. Proto je nutné řešit její kombinace s ostatními bezpečnostními prvky. V České republice již existuje řada firem, které tyto přístupové systémy nabízí, je pouze otázkou vývoje právního prostředí pro podnikatele nakolik se jejich objem bude v budoucnosti zvyšovat.

Použitá literatura

[1] BOHÁČEK, Petr. *Systémy AFIS a rozpoznávání otisků prstů*. [s.l.], 2005. 10 s. VÚT Brno - Fakulta Informačních technologií. Semestrální práce.

[2] BOSH Security Systems [online]. IP produkty - HW. 2008. Dostupný z www: <http://bosch-securitysystems.cz/produkty.php?sel_skup=178#>.

[3] BROMBA, Manfred. *BIOIDENTIFICATION* [online]. 2007 [cit. 2007-11-10]. Dostupný z WWW: <http://www.bromba.com>

[4] CONET [online]. Přístupové systémy. 2001. Dostupný z www: <http://www.conet.cz/pristupove_systemy.html>

[5] ČSN EN 50131-1: *Poplachové systémy - Elektrické zabezpečovací systémy. Část 1: Všeobecné požadavky,* 1999, Změna Z7:2008, Český normalizační institut

[6] ČSN EN 50133-1: *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Část 1: Systémové požadavky,* 2001, Změna A1:2003, Český normalizační institut.

[7] ČSN P ENV 1627: *Okna, dveře, uzávěry - odolnosti proti násilnému vniknutí. Požadavky a klasifikace,* 2000. Český normalizační institut

[8] *FBI Biometric: Center of Excellence* [online]. [1995] [cit. 2007-12-11]. Dostupný z www: <http://www.fbibiospecs.org/fbibiometric/biospecs.html>.

[9] GALBAVÝ, Martin. *Vizualizace a vzdálené řízení v síti LonWorks*. [s.l.], 2006. 61 s. České vysoké učení technické v Praze - Fakulta elektrotechnická. Bakalářská práce.

[10] JABLOTRON [online]. Detektory. 2005. Dostupný z www: <http://www.jablotron.cz/ezs.php?pid=products/ja-60p>

[11] JAIN, Anil, BOLLE, Ruud, PANKANTI, Sharath: *BIOMETRICS - Personal Identification in Networked Society*. London : Kluwer Academic Publisher, 2002. 422 s. ISBN 0-792-38345-1.

[12] MUL-T-LOCK [online]. Mechanické zabezpečovací systémy. 2006. Dostupný z www: <http://www.multlock.cz/cz/kategorie/produkty>

[13] NSTC Subcommittee: *Biometrics Foundation Documents*. [s.l.] : [s.n.], [200-?]. 167 s.

[14] SANDSTROM, Marie: *Liveness Detection in Fingerprint Recognition Systems*. Linkoping, 2004. 149 s.

[15] SAPELI [online]. Dveře a zárubně. 2006. Dostupný z www: <http://www.sapeli.cz/index.asp?obsah=15&amp>

[16] SOUMAR, C. *Biometric system security*. In *Secure*. [s.l.] : [s.n.], 01/2002. s. 46-49.

[17] ŠČUREK, R.: *Přednášky z předmětu Ochrana objektů.* 2007.

[18] UHLÁŘ, J.: *Technická ochrana objektů, I. díl, Mechanické zábranné systémy.* Praha, 2001. ISBN 80-7251-172-6.

[19] UHLÁŘ, J.: *Technická ochrana objektů, II. díl, Elektrické zabezpečovací systémy.* Praha, 2001. ISBN 80-7251-076-2

[20] VANĚK, Richard. *Technologie digitálního snímání prstů*. [s.l.], 2007. 37 s. Univerzita Tomáše Bati ve Zlíně - Fakulta aplikované informatiky. Bakalářská práce.

[21] Zákon č.1/1993 Sb., *Ústava České republiky*

[22] Zákon č.2/1993 Sb., *Listina základních práv a svobod*

[23] Zákon č.29/2000 Sb., *O ochraně osobních údajů*, ve znění pozdějších předpisů a změn

[24] Zákon č.140/1961 Sb., *Trestní zákon*, ve znění pozdějších předpisů a změn

[25] Zákon č.141/1961 Sb., *O trestním řízení soudním*, ve znění pozdějších předpisů a změn

[26] Zákon č.283/1991 Sb., *O Policii České republiky*, ve znění pozdějších předpisů a změn

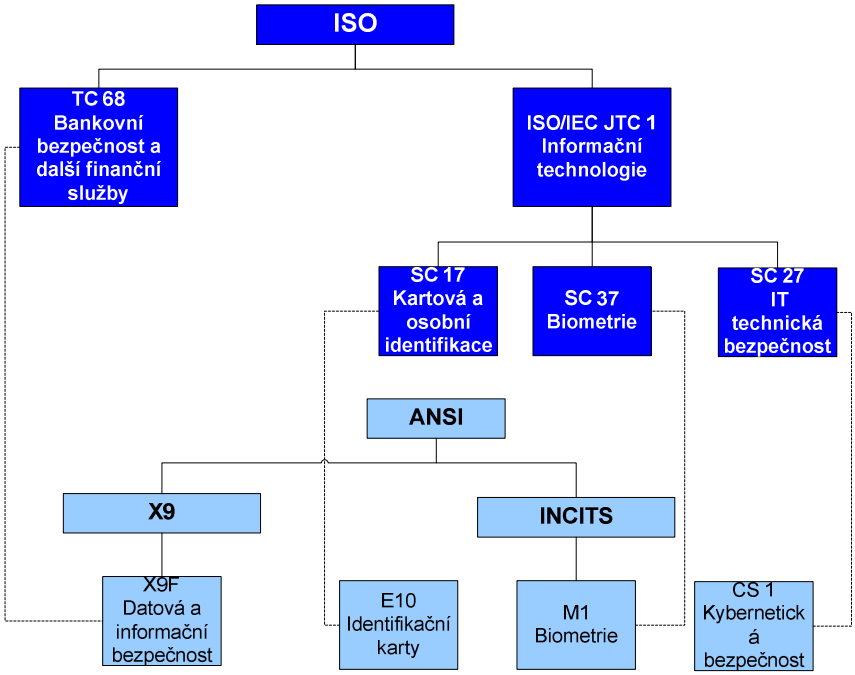
[27] Zákon č. 412/2005 Sb., *O ochraně utajovaných informacích a bezpečnostní způsobilosti*, ve znění pozdějších předpisů a změn

Seznam zkratek

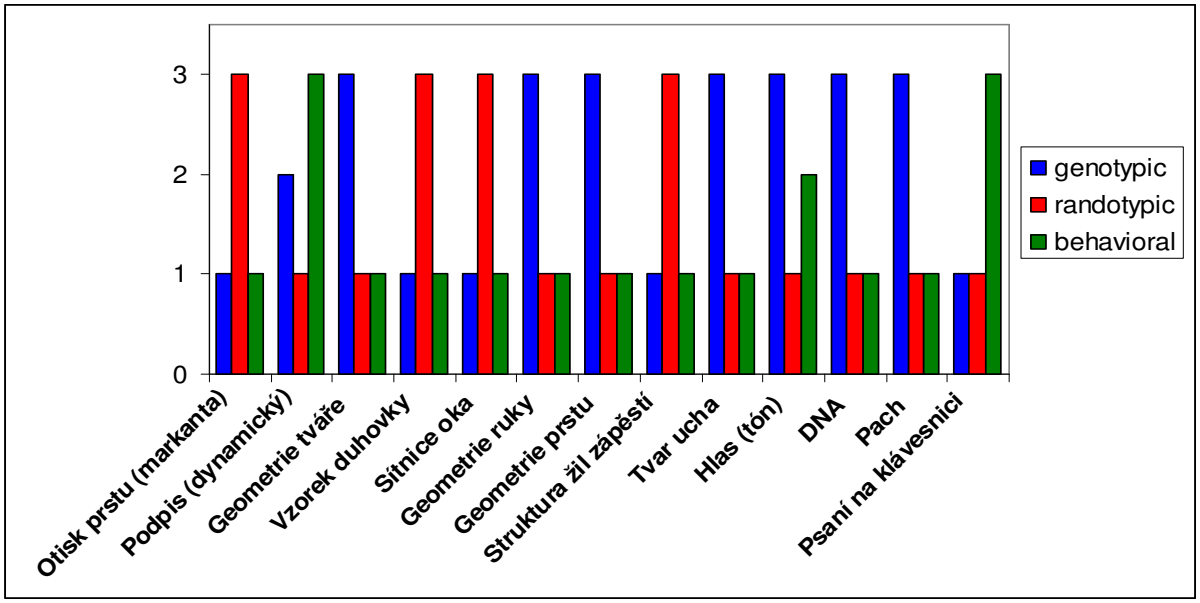
ACS	Access Control Systems - Systémy řízení a kontroly vstupů
AFIS	Automated Fingerprint Identification System - Automatický systém identifikace dle otisku prstu
ANSI	American National Standards Institute - Americký národní standardizační ústav
CCD	Charged Coupled Device - Zařízení s nábojovou vazbou
CCTV	Closed Circuit TV - Uzavřený televizní okruh
CMOS	Complementary Metal Oxide Semiconductor - Polovodič s vrstvou kysličníku křemíku
DIN	Deutsches Institut für Normung - Německý normalizační ústav
DNA	Deoxyribonucleonicacid - Deoxyribonukleová kyselina
EBGM	Elastic bunch graph matching - Elastický srovnávací diagram
FAR	False Acceptance Rate - Koeficient nesprávného přijetí
FIR	False Identification Rate - Koeficient nesprávné identifikace
FMR	False Match Rate - Koeficient nesprávného rozpoznání
FNMR	False None-Match Rate - Koeficient nesprávné nerozpoznání
FRR	False Rejection Rate - Koeficient nesprávného odmítnutí
FTA	Failure To Acquire - Koeficient selhání přístupu
FTA	Fault Tree Analysis - Analýza stromem poruch
IEC	International Electrotechnical Commision - Mezinárodní komise pro elektrotechniku
INCITS	International Committee for Information Technology Standards - Mezinárodní komise pro standardizaci informačních technologií
ISO	International Organization for Standardization - Mezinárodní organizace pro standardizaci
OASIS	Organization for the Advancement of Structured Information Standards - Organizace pro rozvoj strukturovaných informačních standardů
PIR	Pasive Infrared - Pasivní infračervené čidlo
TFT	Thin Film Transistor - Tenkovrstvý tranzistor

Seznam příloh:

Příloha č.1: Subordinace a spolupráce orgánů při tvorbě technických norem ve světě



Příloha č.2: Vliv vývojových vlastností na jednotlivé biometrické znaky a jejich porovnání



Příloha č. 2/1: Relativní vliv vývojových vlastností na jednotlivé biometrické znaky

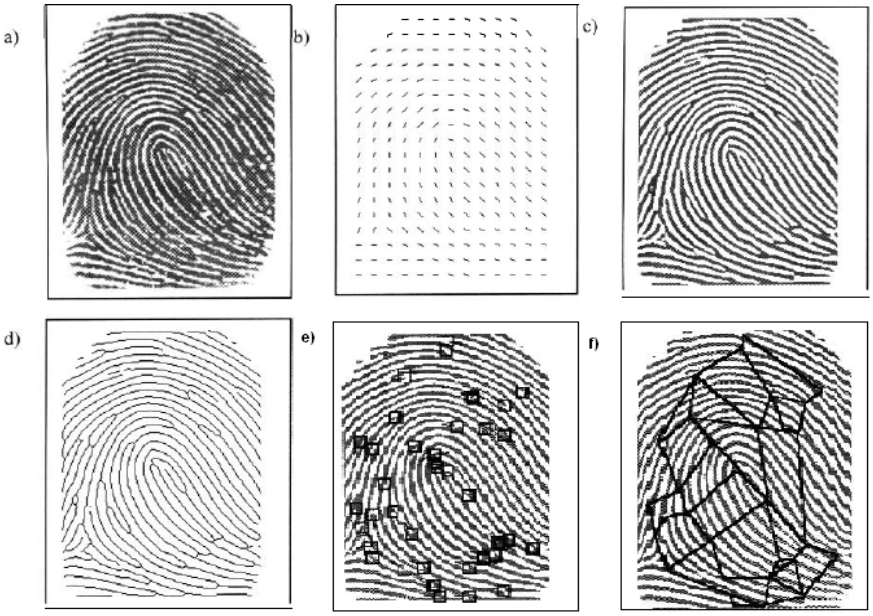
Biometrická vlastnost	komfort	přesnost	dostupnost	cena
Otisk prstu	ooooooo (7)	ooooooo (7)	oooo (4)	ooo (3)
Podpis (dynamický)	ooo (3)	oooo (4)	ooooo (5)	oooo (4)
Geometrie tváře	oooooooo (9)	oooo (4)	ooooooo (7)	ooooo (5)
Vzorek duhovky	oooooooo (8)	oooooooo(9)	oooooooo (8)	oooooooo (8)
Sítnice oka	oooooo (6)	oooooooo (8)	ooooo (5)	ooooooo (7)
Geometrie ruky	oooooo (6)	ooooo (5)	oooooo (6)	ooooo (5)
Geometrie prstu	ooooooo (7)	ooo (3)	ooooooo (7)	oooo (4)
Struktura žil zápěstí	oooooo (6)	oooooo (6)	oooooo (6)	ooooo (5)
Tvar ucha	ooooo (5)	oooo (4)	ooooooo (7)	ooooo (5)
Hlas (tón)	oooo (4)	oo (3)	ooo (3)	oo (2)
DNA	o (1)	ooooooo (7)	oooooooo(9)	oooooooo(9)
Pach	?	oo (2)	ooooooo (7)	?
Psaní na klávesnici	oooo (4)	o (1)	oo (2)	o (1)
Srovnání: heslo	ooooo (5)	oo (2)	oooooooo (8)	o (1)

zelená = nejlepší; červená = nejhorší

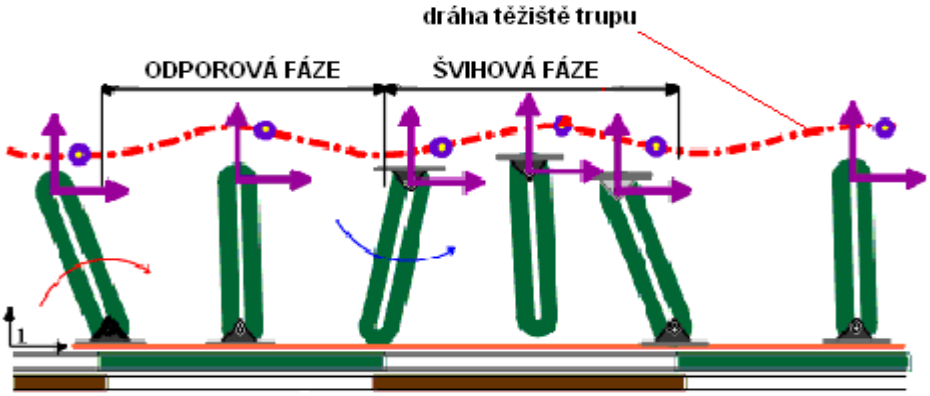
Příloha č.2/2: Porovnání jednotlivých biometrických vlastností

Příloha č.3: Seskupení papilárních linií, tvorba markantografu a princip bipedální lokomoce

Příloha č.3/1: Ukázka tří hlavních seskupení papilárních linií

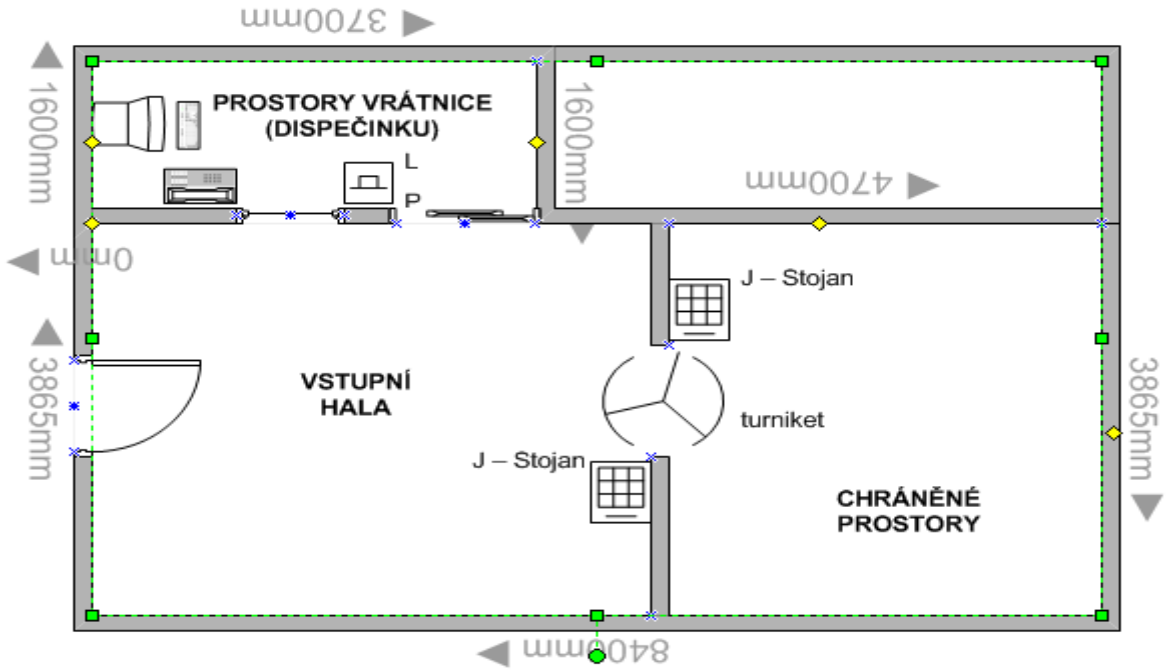


Příloha č.3/2: a) originální otisk b) filtr orientace markant
c) binarizace d) zeslabení e) nalezení markant f) markantograf

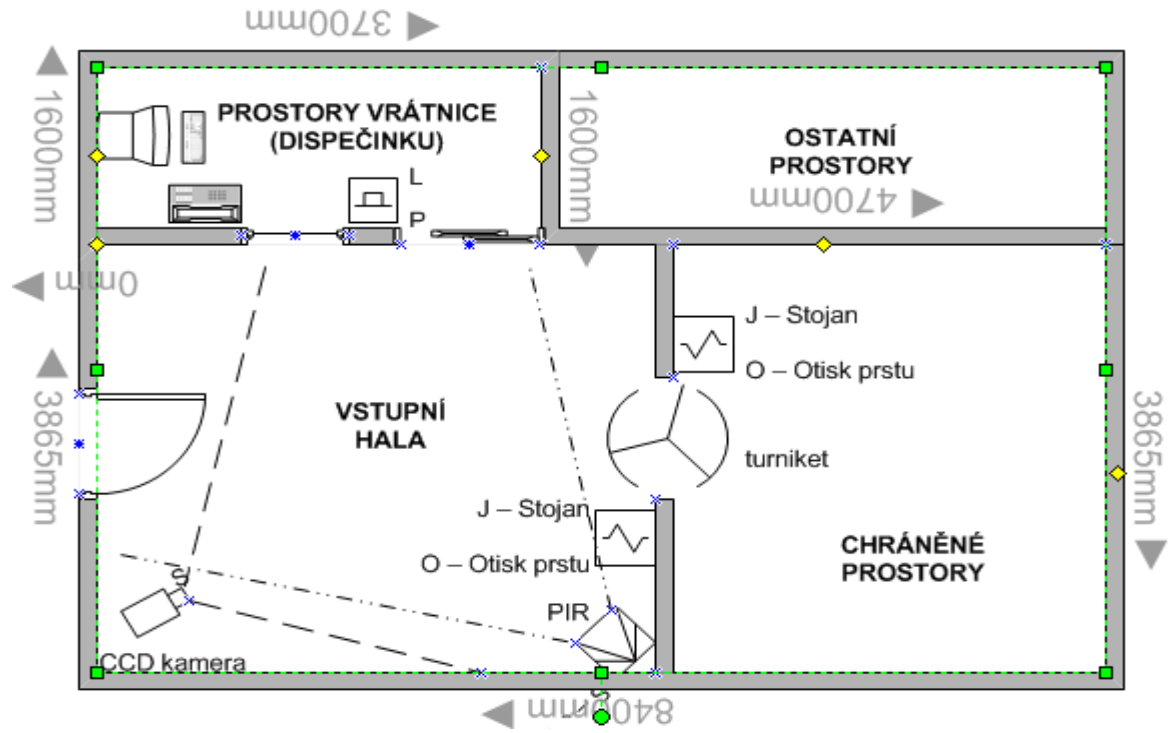


Příloha č.3/3: Postup vytváření dráhy těžiště trupu při bipedální lokomoci

Příloha č.4: Situační schéma vstupních prostor a schéma pokrytí kamery a PIR čidla

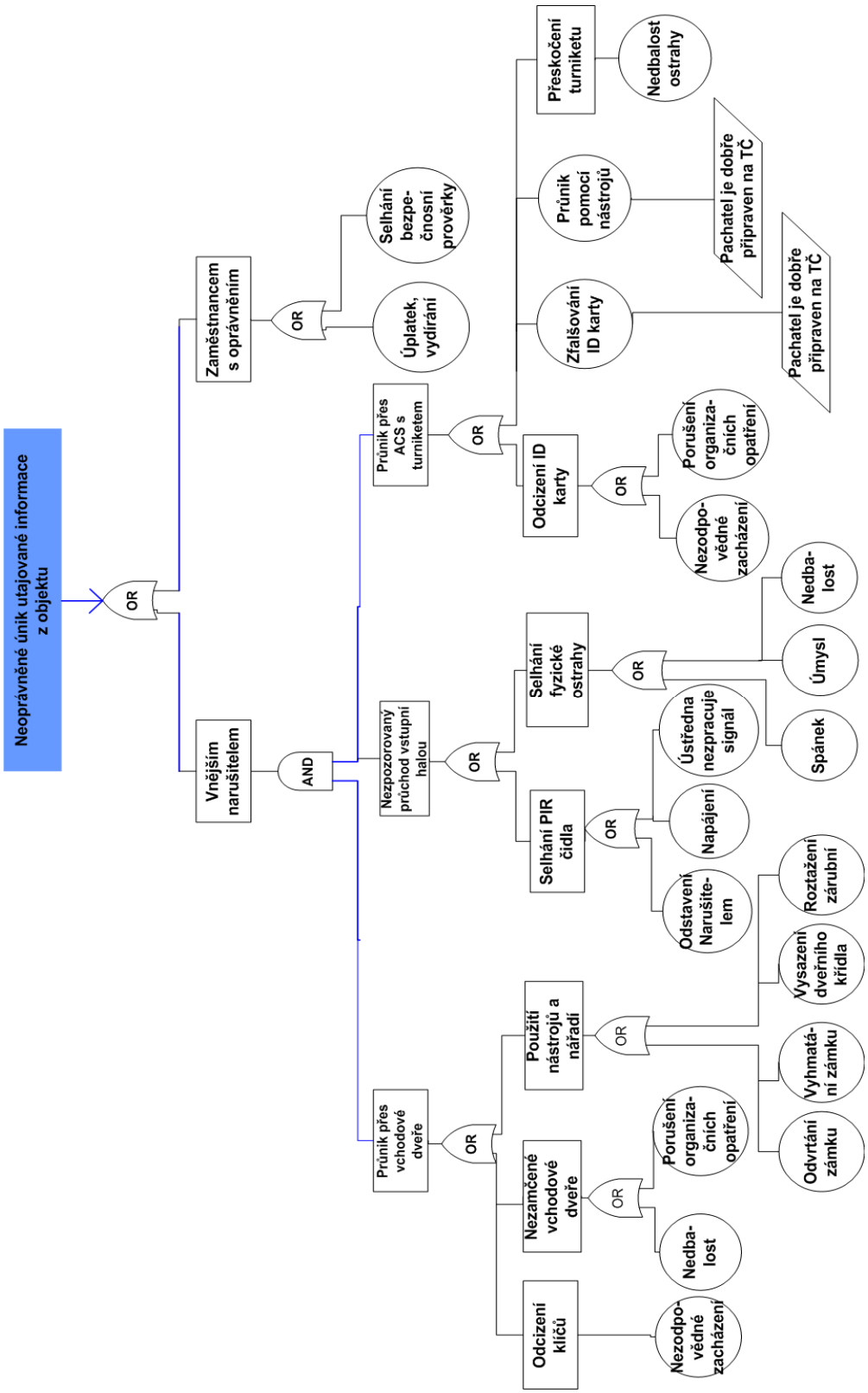


Příloha č. 4/1: Situační schéma vstupních prostor se stávajícím zabezpečením



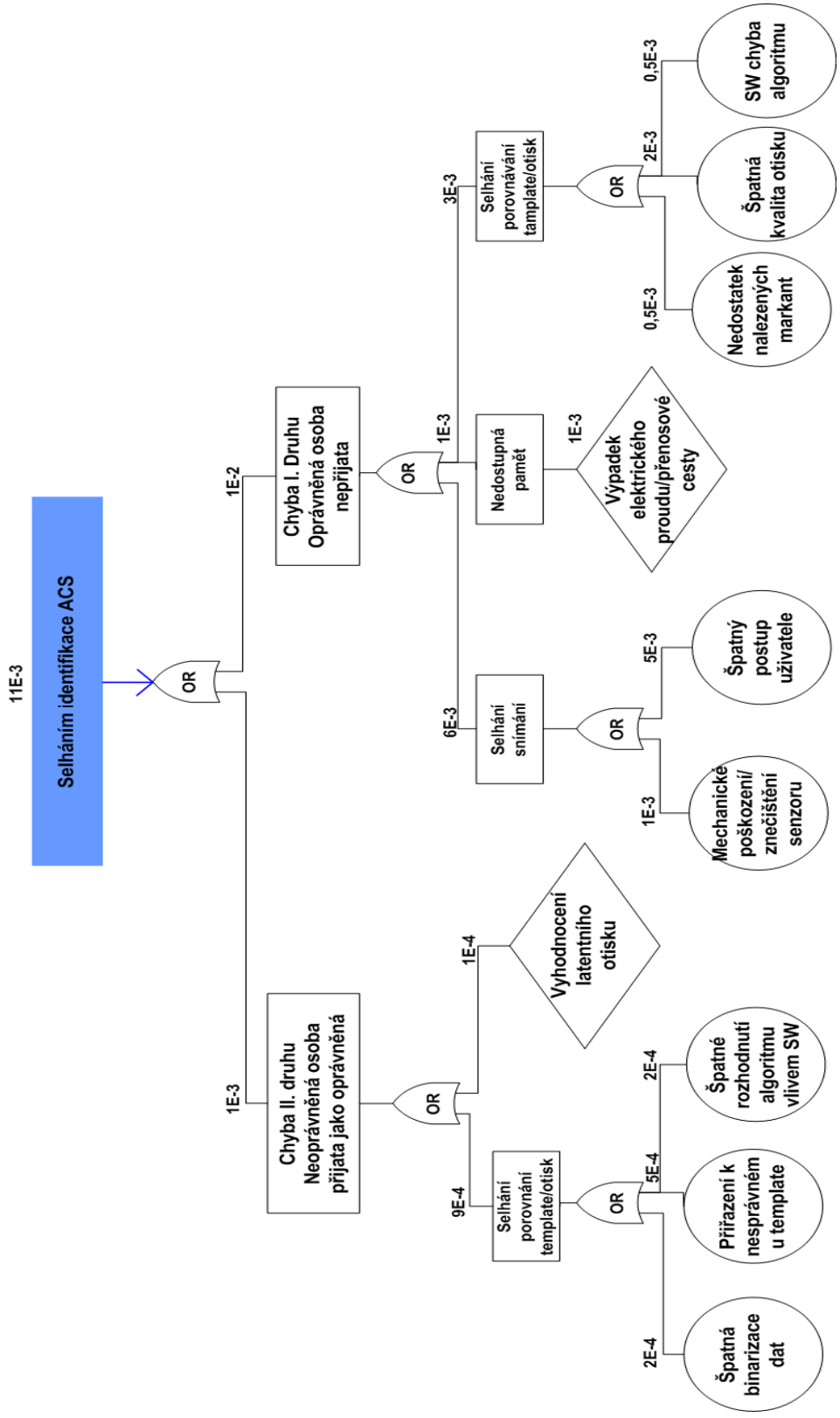
Příloha č. 4/2: Prostorové pokrytí kamery a PIR čidla

Příloha č.5/1: Modelování rizika pomocí FTA



Příloha č. 5/1: FTA pro neoprávněný únik utajované informace

Příloha č.5/2: Modelování rizika pomocí FTA s výpočtem pravděpodobnosti



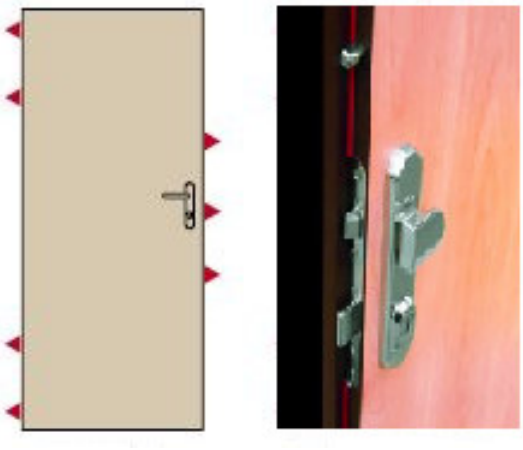
Příloha č. 5/2: FTA pro selhání ACS

Příloha č.6: Tabulka analýzy FMEA možných příčin poruch a jejich následků z hlediska strukturálního

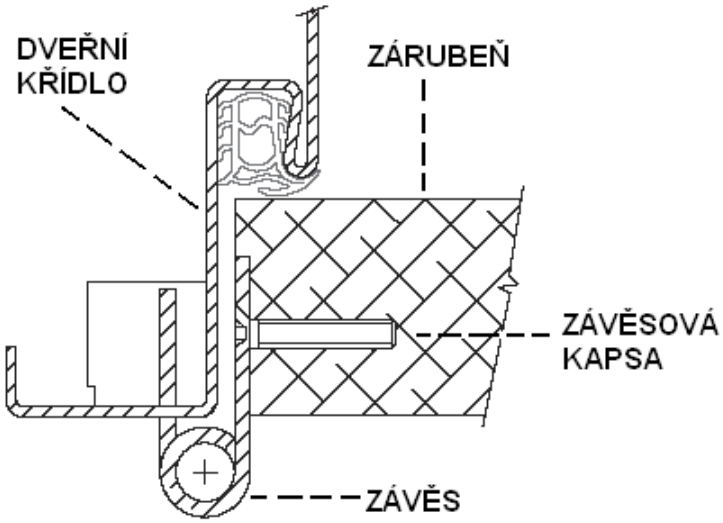
Objekt	Subsystém	Identifikace nebezpečí	P	N	H	R	Současný stav	P	N	H	R	Nový stav	Kontrola	Příčiny	Následky
VSTUPNÍ PROSTORY DO OBJEKTU	HLAVNÍ VCHOD	1. Neoprávněný průnik do vstupní haly	3	3	4	36	Mechanické zábranné systémy	2	3	1	6	Kvalitnější MZS v kombinaci s EZS	Kontrola stavu dveří	Nedostatečné MZS a kontrola	Průnik do vstupní haly
		2. Vyhmatání zámku	4	3	5	60	Nevyhovující zámek, cylindrická vložka i kování	1	3	4	12	Bezpečnostní rozvorový zámek	Kontrola mechanického poškození zámku	Primitivní zámek i vložka	Průnik přes dveře
		3. Odvrtání zámku	4	3	3	36	Nevyhovující zámek, cylindrická vložka i kování	1	3	2	6	Bezpečnostní rozvorový zámek	Kontrola mechanického poškození zámku	Primitivní zámek i vložka	Průnik přes dveře
		4. Vypáčení dveřního křídla ze závěsů	4	4	2	32	Klasické nevyhovující 1-osově otočné závěsy	2	4	2	16	3D otočné závěsy	Kontrola mechanického poškození	Závěsy otočné po jedné ose	Průnik přes dveře
		5. Roztažení zárubní	3	4	2	24	Klasické vybetonované zárubně						Kontrola mechanického poškození	Překonání mechanické odolnosti zárubní	Průnik přes dveře
		6. Vybourání těžkými nástroji, vozidlem	2	4	1	9	Železobetonová zděná konstrukce objektu						Kontrola mechanického poškození	Překonání mechanické odolnosti dveří	Průnik přes dveře
		7. Překonání složitými nástroji	2	4	1	9	Hluk musí registrovat FO						Kontrola mechanického poškození	Překonání mechanické odolnosti dveří	Průnik přes dveře
	PROSTORY VSTUPNÍ HALY	8. Pohyb nežádoucích osob v prostorách haly a přístup k ACS	4	4	2	32	Analogové PIR čidlo, nevyhovující ústředna EZS, FO externí službou	3	4	1	12	Lepší čidla, ústředna i FO	Kontrola stavu a funkčnosti EZS, kamery	Nedostatečné zabezpečení	Možnost manipulace s ACS, PIR…
		9. Sabotáž PIR čidla	3	4	4	48	Nevyhovující PIR čidlo bez tamperu	2	4	1	8	Digitální PIR s ochranou proti sabotáži	Samokontrola tamperem, kontrola ústřednou EZS	Manipulace s PIR čidlem, clonou	Deaktivace PIR čidla - volný pohyb
		10. Útok na fyzickou ostrahu	3	4	2	24	Externí zaměstnanec FO se základním výcvikem						Školení, pravidelný výcvik, popř. vlastní FO	Útočník	Eliminace fyzické ochrany
		11. Vniknutí do ventilačních šachet	3	4	4	48	Žádná opatření	2	4	1	8	Rozpěrná tyč s kontakty na EZS	Kontrola kontaktů ústřednou, člověkem	Volný vstup do chráněných prostor	Průnik do chráněných prostor
		12. Založení požáru	2	5	2	20	Instalována EPS							Zkrat, porucha, úmysl	Škody na majetku, ohrožení osob
	SYSTÉM ŘÍZENÍ A KONTROLY VSTUPŮ	13. Neoprávněný vstup osob do chráněných prostor	4	5	3	60	ACS systém s kartovou ID identifikací, nízký turniket	1	5	2	10	Biometrický ACS, vysoký plný turniket	Kontrola kamerou, PIR čidlem, FO	Nedostatečná autentizace	Narušení chráněných prostor
		14. Přelezení nízkého turniketu	4	5	3	60	Dohled FO	1	5	1	5	Vysoký plný turniket	Bez kontroly - vysoký turniket nelze přelézt	Nedostatečná překážka	Vniknutí do prostor
		15. Zneužití odcizené ID karty	2	5	3	30	Hlášení ztracených ID karet, nevyhovující	1	5	2	10	Biometrická autentizace namísto vlastnictví tokenu	Systém kontroluje pokusy o přístup, téměř nemožné odcizení bio. vlastnosti	Autentizace vlastnictvím tokenu	Vniknutí do chráněných prostor
		16. Zásah do systému ACS	3	4	3	36	Dohled FO	2	5	2	20	Dohled FO, kamerou, lepší ACS	Kontrola kamerou, FO	Nedostatečná kontrola	Narušení systému ACS
		17. Přístup falšováním ID karty	4	5	4	80	Žádná opatření	1	5	2	10	Biometrická autentizace	Kontrola uživatelů databáze	Nedostatečné zabezpečení	Vniknutí do prostor
		18. Výpadek elektrického proudu	2	5	1	10	Náhradní zdroje elektrické energie UPS pro EZS a EPS						Pravidelné kontroly a revize	Zkrat, přerušení dodávky	Vyřazení bezpečnostních prvků
		19. Vniknutí do systému ACS a zneužití uložených dat	2	4	4	32	Dohled FO	1	4	2	8	Centrální ukládání dat v PC	Kontrola komunikace na lince proti útokům na IS	Ukládání přímo v zařízení, snímači	Zneužití identifikačních dat

Příloha č. 6: Tabulka FMEA analýzy

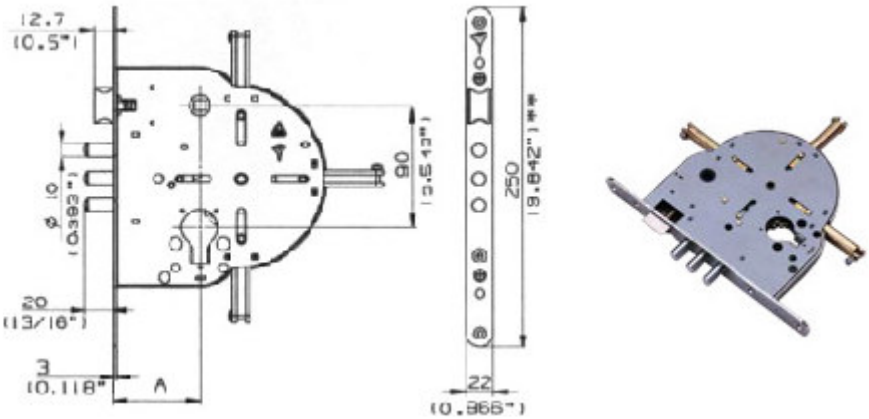
Příloha č.7: Prvky navrhovaného mechanického zábranného systému - dveřní křídlo, závěs, zámek



Příloha č. 7/1: Schématický náčrt umístění čepů a reálný výřez ve dveřním křídle SAPELI

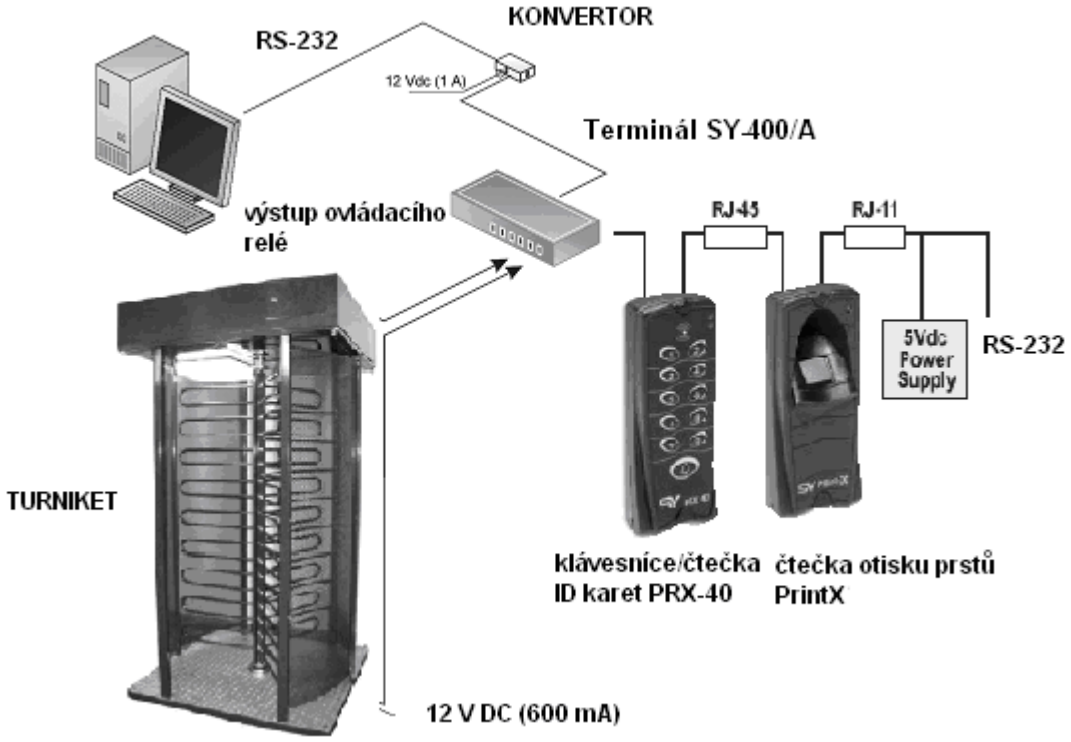


Příloha č. 7/2: Ukotvení 3D seřiditelných závěsů Simonswerk v řezu

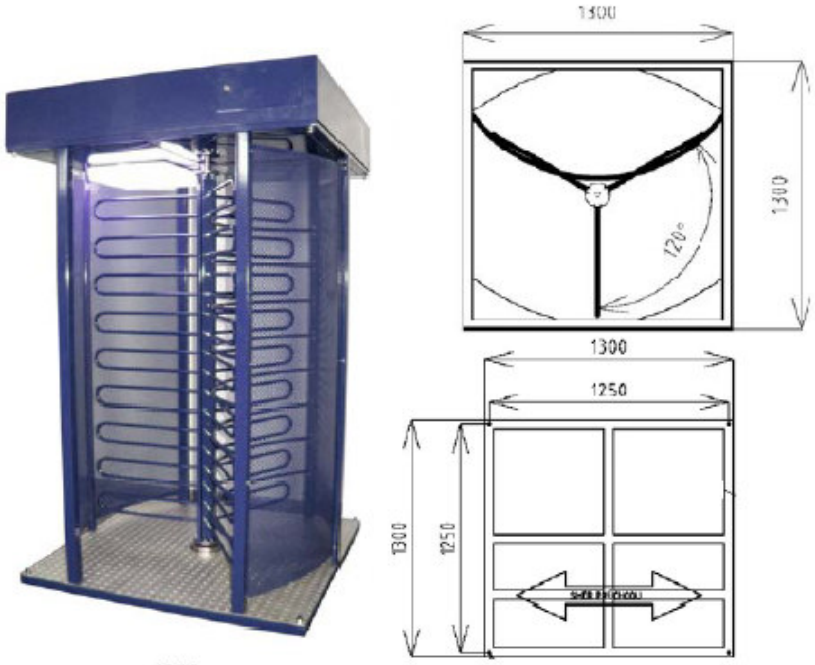


Příloha č. 7/3: Detail rozvorového zámku MUL-T-LOCK

Příloha č.8: Zapojení biometrické přístupového systému Synel s turniketem AUTOGARD



Příloha č. 8/1: Blokové schéma zapojení přístupového systému Synel



Příloha č. 8/2: Turniket AUTOGARD ATF 600 a jeho rozměry

Příloha č.9: Technická data biometrického snímače otisků prstů Synel PrintX

Technologie snímání	kapacitní
Kapacita paměti	4000 uživatelů
Velikost šablony (template)	350 B = 2800 b
Dostupná nastavení bezpečnosti	very high, high, average, low, very low
FAR	< 0,001
EER	0,001
FAR/FRR	0,003
Doba ověřování	< 1 sekund
Doba záznamu	< 5 sekund
Rozlišení senzoru	300 x 300 pixelů
Plocha senzoru	1,5 cm^2
Pracovní teplota	-10 °C až + 50 °C
Relativní vlhkost	95%
Komunikace - asynchronní	9600 b/s; TTL rozhraní
Napájení	5 V=
Přípustná rotace prstu	+/- 18°
Přípustné posunutí prstu	+/- 5 mm
Váha	180 g
Velikost	130 x 43 x 20 mm

Příloha č. 9: Technická data biometrického snímače otisku prstů Synel PrintX